COMTREND CORPORATION

AR-5389

ADSL2+ WLAN Router

User Manual

Version A1.0, February 5, 2014

Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix B - Specifications.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Copyright

Copyright© 2014 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

NOTE:	This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

Table of Contents

CHAPTER 1 INTRODUCTION 6

CHAPTER 2 INSTALLATION 7

2.1 HARDWARE SETUP 7

2.2 FRONT PANEL 9

CHAPTER 3 WEB USER INTERFACE 11

3.1 DEFAULT SETTINGS 11

3.2 IP CONFIGURATION 11

3.3 LOGIN PROCEDURE 14

CHAPTER 4 DEVICE INFORMATION 16

4.1 WAN 17

4.2 STATISTICS 18

4.2.1 LAN Statistics 18

4.2.2 WAN Service Statistics 19

4.2.3 xTM Statistics 20

4.2.4 xDSL Statistics 21

4.3 ROUTE 25

4.4 ARP 26

4.5 DHCP 27

4.5.1 DHCPv4 27

4.5.2 DHCPv6 28

4.6 NAT SESSION 29

4.7 IGMP PROXY 30

4.8 IPV6 31

4.8.1 IPv6 Info 31

4.8.2 IPv6 Neighbor 32

4.8.3 IPv6 Route 33

CHAPTER 5 ADVANCED SETUP 34

5.1 LAYER 2 INTERFACE 34

5.1.1 ATM Interface 34

5.1.2 PTM Interface 34

5.1.3 ETH Interface 35

5.2 WAN SERVICE 36

5.3 LAN 37

5.3.1 LAN IPv6 Autoconfig 40

5.3.2 Static IP Neighbor 43

5.4 AUTO-DETECTION 44

5.5 NAT 48

5.5.1 Virtual Servers 48

5.5.2 Port Triggering 50

5.5.3 DMZ Host 52

5.5.4 IP Address Map 53

5.5.5 IPSEC ALG 55

5.5.6 SIP ALG 56

5.6 SECURITY 57

5.6.1 IP Filtering 57

5.6.2 MAC Filtering 60

5.7 PARENTAL CONTROL 62

5.7.1 Time Restriction 62

5.7.2 URL Filter 63

5.8 QUALITY OF SERVICE (QOS) 65

5.8.1 Queue Management Configuration 65

5.8.2 Queue Configuration 66

5.8.3 QoS Policer 68

5.8.4 QoS Classification 70

5.9 ROUTING 73

5.9.1 Default Gateway *73*
5.9.2 Static Route *74*
5.9.3 Policy Routing *75*
5.9.4 RIP *76*
5.10 DNS 77
5.10.1 DNS Server *77*
5.10.2 Dynamic DNS *78*
5.10.3 DNS Entries *80*
5.11 DSL 81
5.12 UPnP 83
5.13 DNS Proxy/Relay 84
5.14 Interface Grouping 85
5.15 IP Tunnel 88
5.15.1 IPv6inIPv4 ..... *88*
5.15.2 IPv4inIPv6 ..... *90*
5.16 IPSec 92
5.17 Certificate 95
5.17.1 Local *95*
5.17.2 Trusted CA *98*
5.18 Multicast 100

CHAPTER 6 WIRELESS 102
6.1 Basic 102
6.2 Security 104
6.2.1 WPS *107*
6.3 MAC Filter 111
6.4 Wireless Bridge 112
6.5 Advanced 113
6.6 Site Survey 116
6.7 Station Info 117
6.8 WiFi Button 118

CHAPTER 7 DIAGNOSTICS 119
7.1 Diagnostics – Individual Tests 119
7.2 Fault Management 120
7.3 Uptime Status 121

CHAPTER 8 MANAGEMENT 122
8.1 Settings 122
8.1.1 Backup Settings *122*
8.1.2 Update Settings *122*
8.1.3 Restore Default *123*
8.2 System Log 124
8.3 SNMP Agent 126
8.4 TR-069 Client 127
8.5 Internet Time 129
8.6 Access Control 130
8.6.1 Accounts/Passwords *130*
8.6.2 Service Access *132*
8.6.3 IP Address *133*
8.7 Update Software 135
8.8 Reboot 136

APPENDIX A - FIREWALL 137

APPENDIX B – SPECIFICATIONS 139

APPENDIX C - SSH CLIENT 142

APPENDIX D - WPS OPERATION 143

APPENDIX E - CONNECTION SETUP 147

Chapter 1 Introduction

The AR-5389 is a wireless ADSL2+ router with an uplink rate of up to 1 Mbps and downlink rate of up to 24 Mbps. It provides one RJ11 telephone interface, four RJ45 Ethernet interfaces, and 802.11b/g/n interface. It is an ideal broadband CPE solution for both home users who wish to share high-speed Internet access and small offices that wish to do business on the Internet.

The AR-5389 has a Web-based graphic user interface (GUI), in which you can easily modify the settings and connect to your ISP. It also provides flow statistics, connection status, and other detailed information. It supports static IP address, dynamic IP address, and PPPoE connection, IPv6 and TR-069.

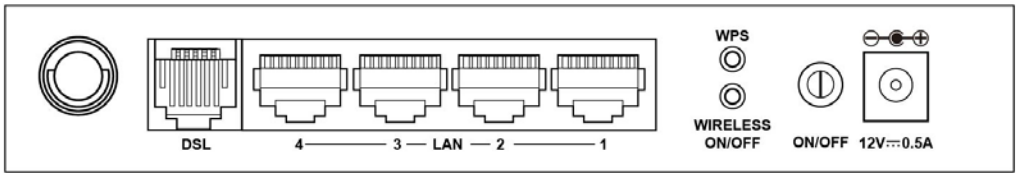
Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



DSL
Connect to the DSL port with the DSL RJ11 cable.

LAN (Ethernet) Ports
You can connect the router to up to four LAN devices using RJ45 cables. The ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

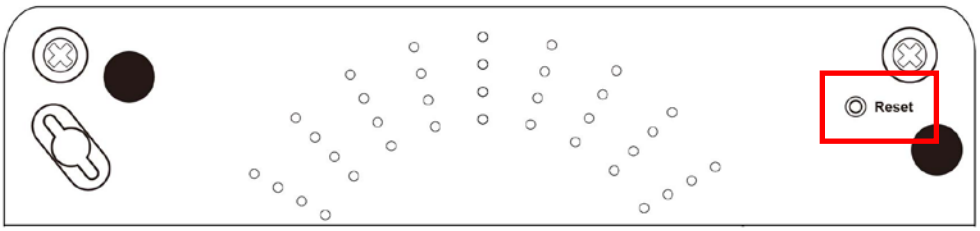
WPS Button
Press this button to begin searching for WPS clients. These clients must also enable WPS push button mode (see 6.2.1 WPS for instructions).

WIRELESS
Press this button to enable/disable the wireless LAN (WLAN).

Power ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section Front Panel – LED Indicators).

Caution 1:	If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.
Caution 2:	Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

BOTTOM PANEL

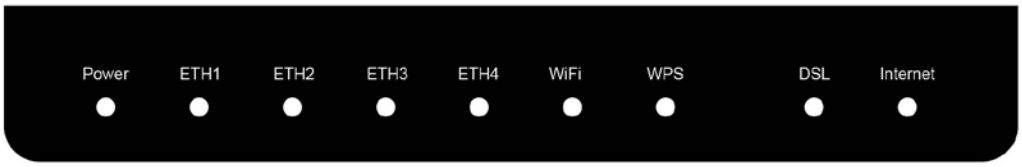


Reset Button
Restore the default parameters of the device by pressing the Reset button for 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.2 Front Panel for details).

NOTE:	If pressed down for more than 60 seconds, the AR-5389 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

2.2 Front Panel

The front panel LED indicators are shown below and explained in the following table. This information can be used to check the status of the device and its connections.



LED	Color	Mode	Function
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
ETH 1X-4X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
WiFi	Green	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WIFI.
WPS	Green	On	WPS function is OK.
		Off	WPS function is closed or failure.
DSL	Green	On	xDSL Link is established.
		Off	Modem power off.
		Blink	fast: xDSL Link is training or data transmitting. slow: xDSL training failed.
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
		Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		Blink	IP connected and IP Traffic is passing through the device (either direction)

Note:

A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.

IP connected (the device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has successfully complete – if used – and DSL is up) and no traffic detected. If the IP or PPPoE session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- WIFI access: **enabled**

Technical Note

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 IP Configuration

DHCP MODE

When the AR-5389 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

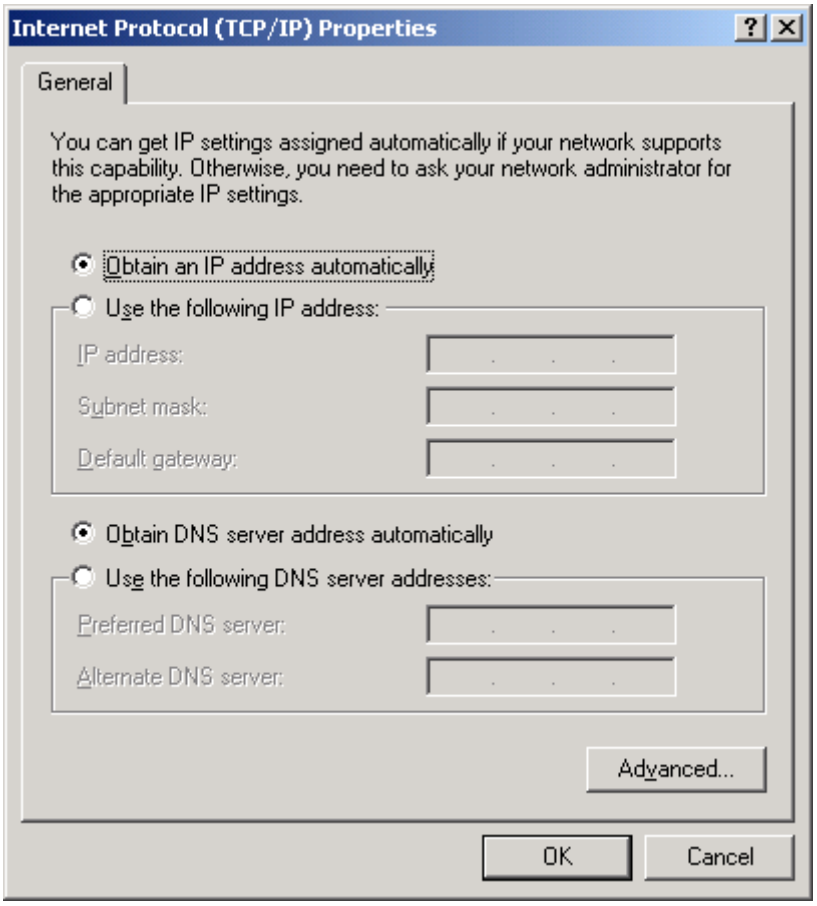
To obtain an IP address from the DCHP server, follow the steps provided below.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Select Obtain an IP address automatically as shown below.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

STEP 4: Click **OK** to submit these settings.

If you experience difficulty with DHCP mode, you can try static IP mode instead.

STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

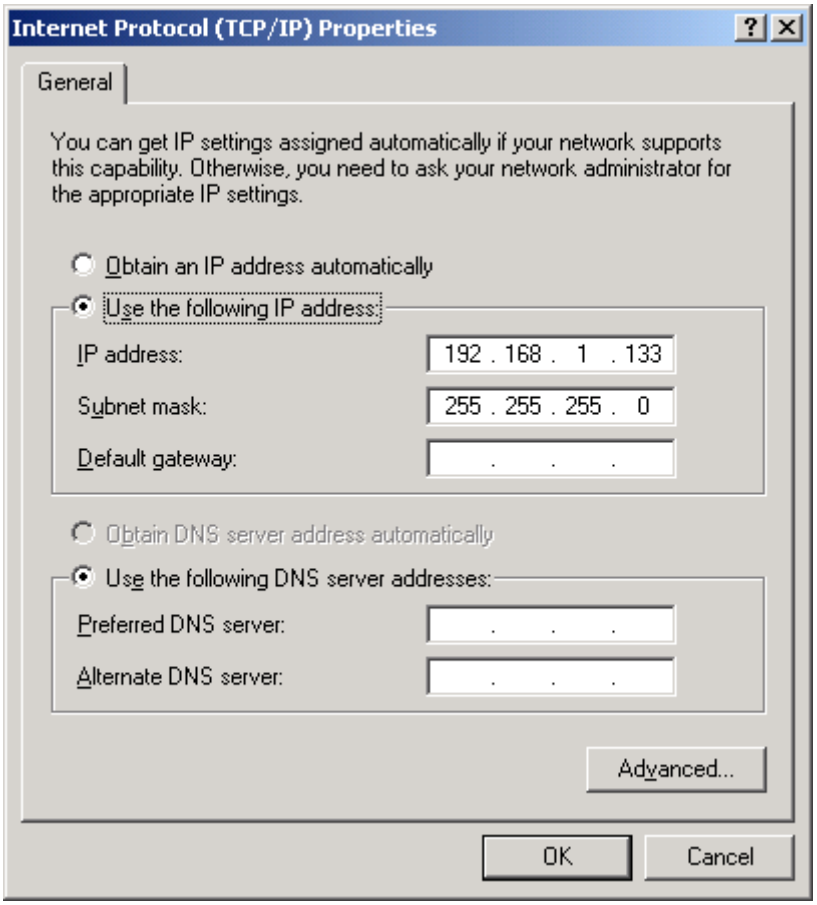
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 133
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

STEP 4: Click **OK** to submit these settings.

3.3 Login Procedure

Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in 3.1 Default Settings.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Chapter 4 Device Information screen and login with remote username and password.

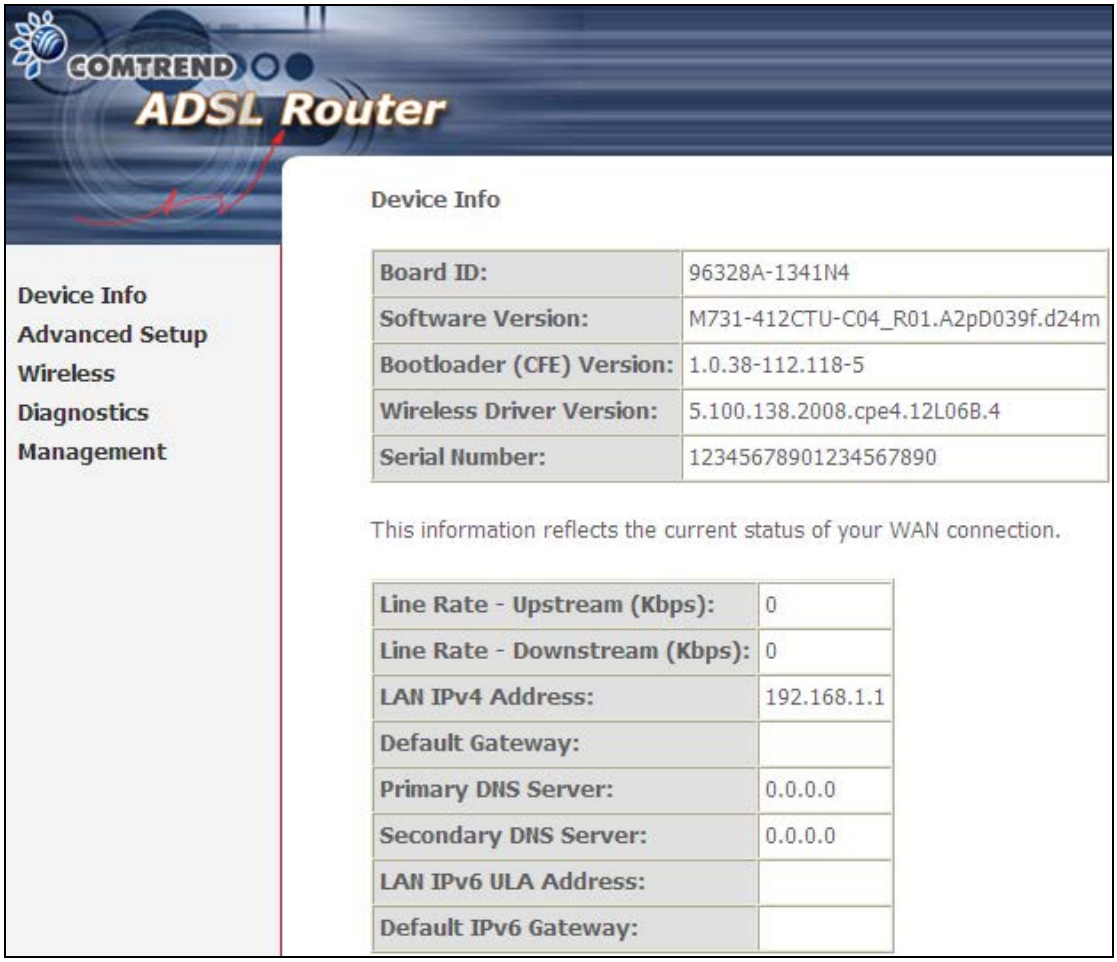
STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.

Connect to 192.168.1.1
The server 192.168.1.1 at DSL Router requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
root
Password:
Remember my password
OK
Cancel

Click **OK** to continue.

NOTE:	The login password can be changed later (see 8.6.1 Passwords).

STEP 3: After successfully logging in for the first time, you will reach this screen.



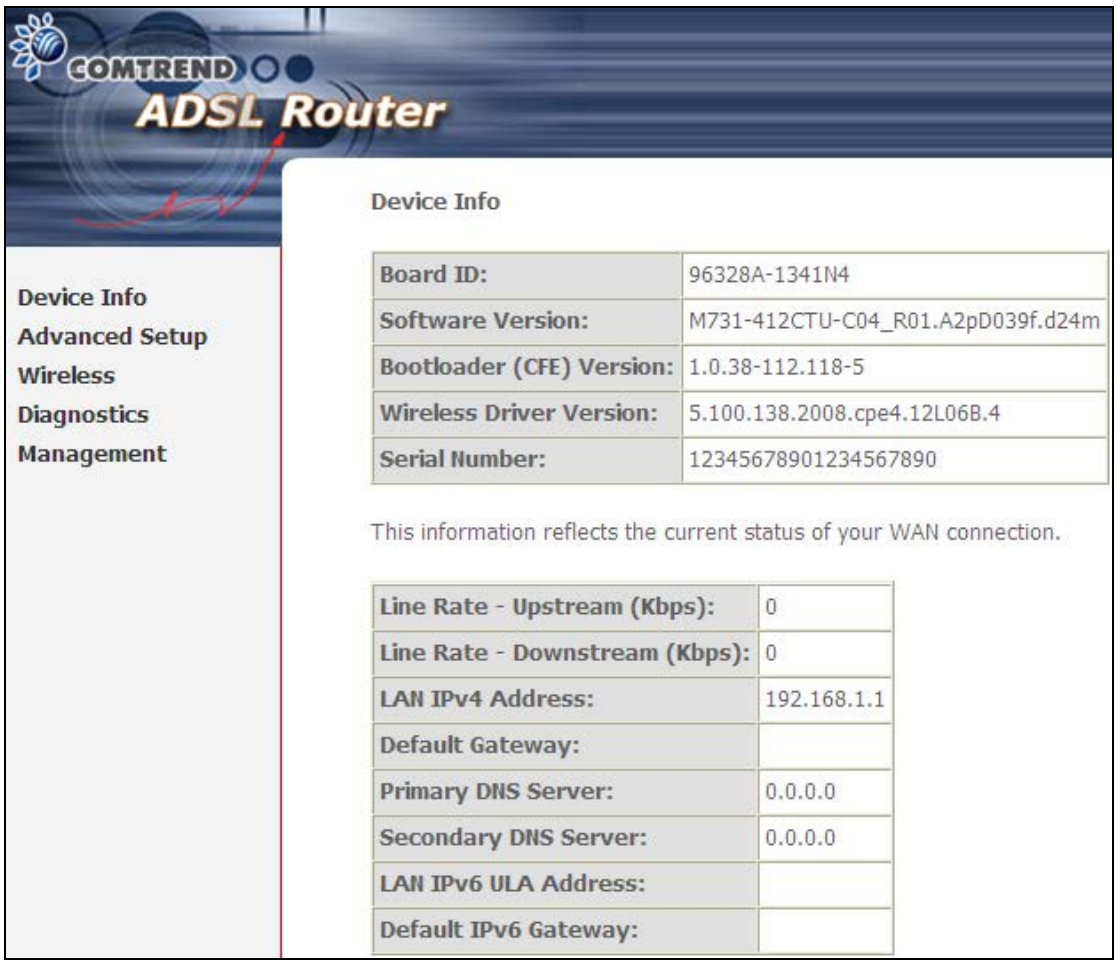
Chapter 4 Device Information

The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

NOTE:	The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

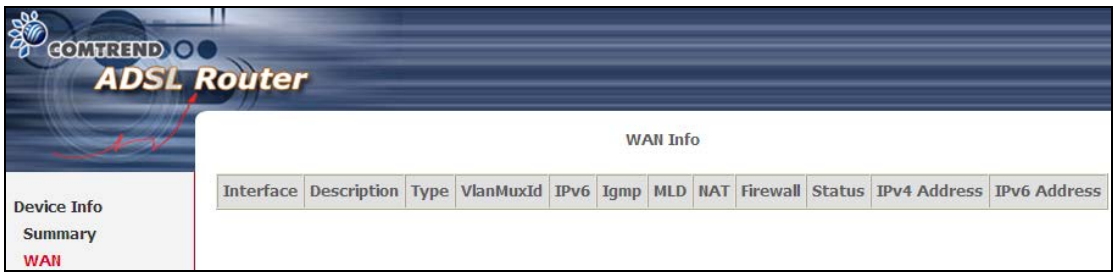
Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

The Device Info Summary screen displays at startup.



4.1 WAN

Select WAN from the Device Info submenu to display the configured PVC(s).



Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IPv6	Shows WAN IPv6 address
IGMP	Shows Internet Group Management Protocol (IGMP) status
MLD	Shows Multicast Listener Discovery (MLD) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address
IPv6 Address	Shows WAN IPv6 address

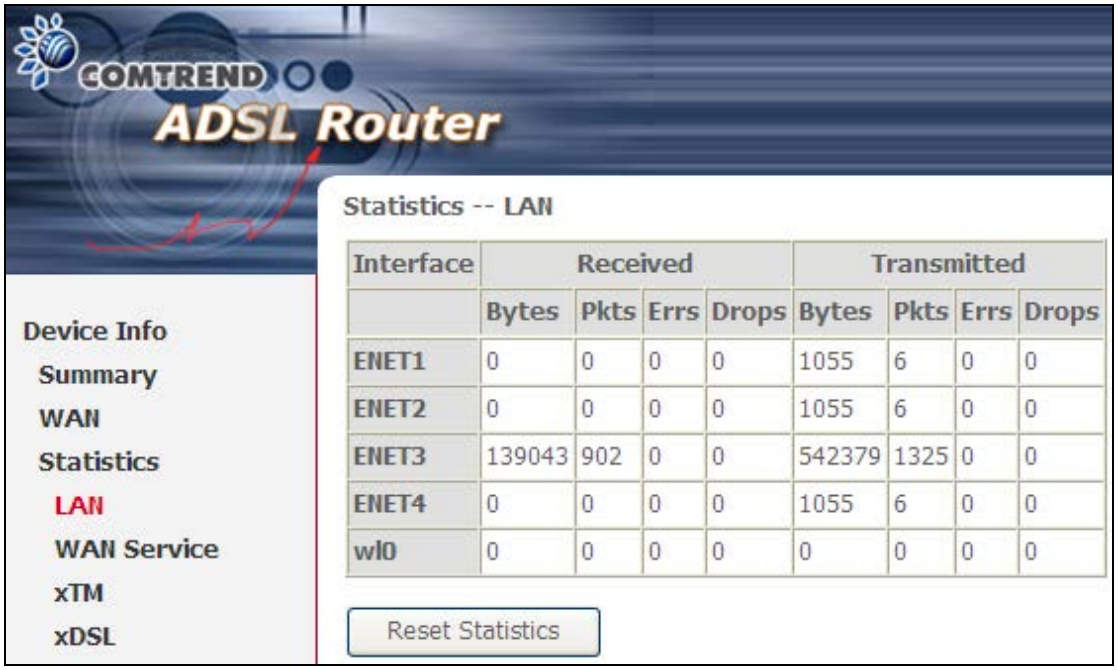
4.2 Statistics

This selection provides LAN, WAN Service, XTM and xDSL statistics.

NOTE:	These screens are updated automatically every 15 seconds. Click **Reset Statistics** to perform a manual update.

4.2.1 LAN Statistics

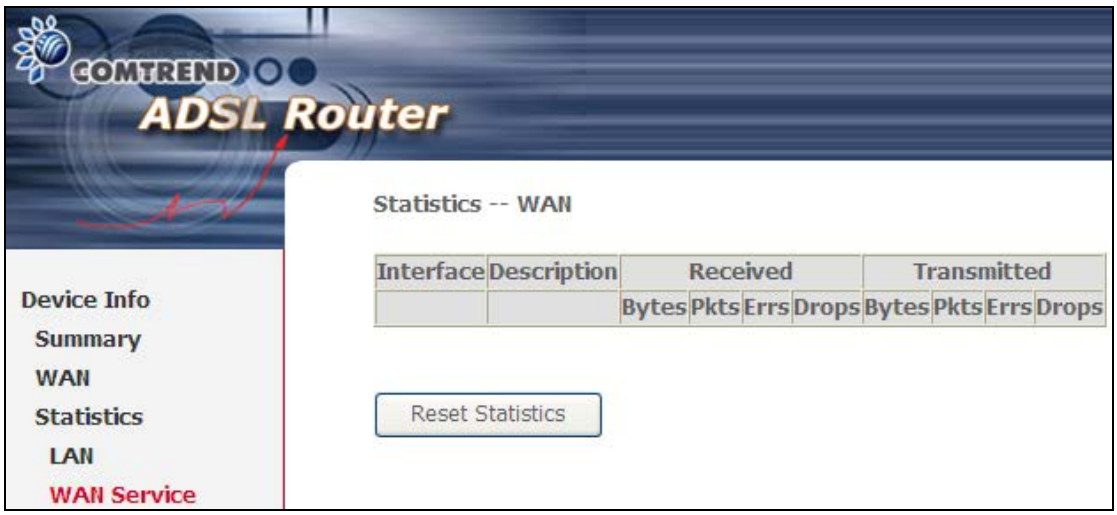
This screen shows data traffic statistics for each LAN interface.



Heading	Description
Interface	LAN interface(s)
Received/Transmitted: - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.2 WAN Service Statistics

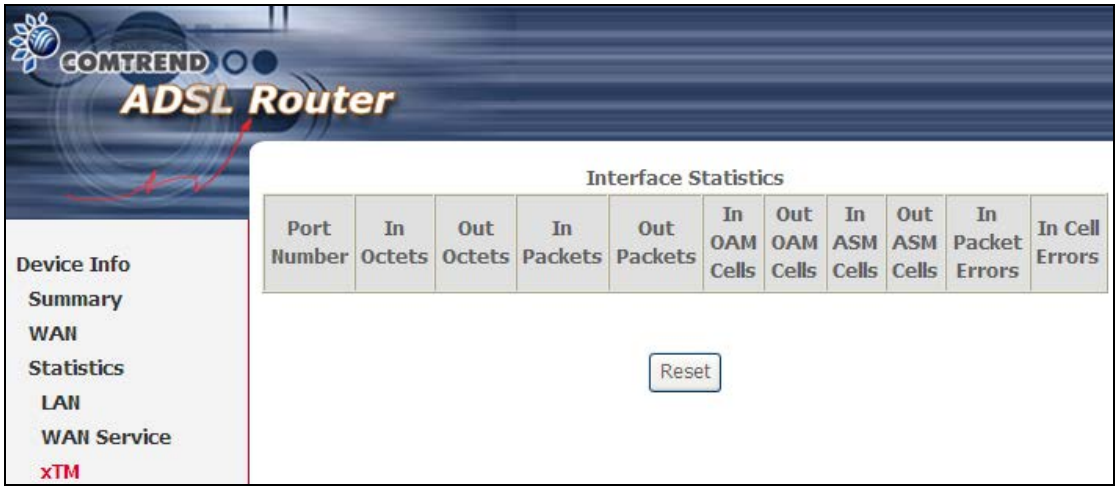
This screen shows data traffic statistics for each WAN interface.



Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.3 xTM Statistics

The following figure shows Asynchronous Transfer Mode (xTM) statistics.



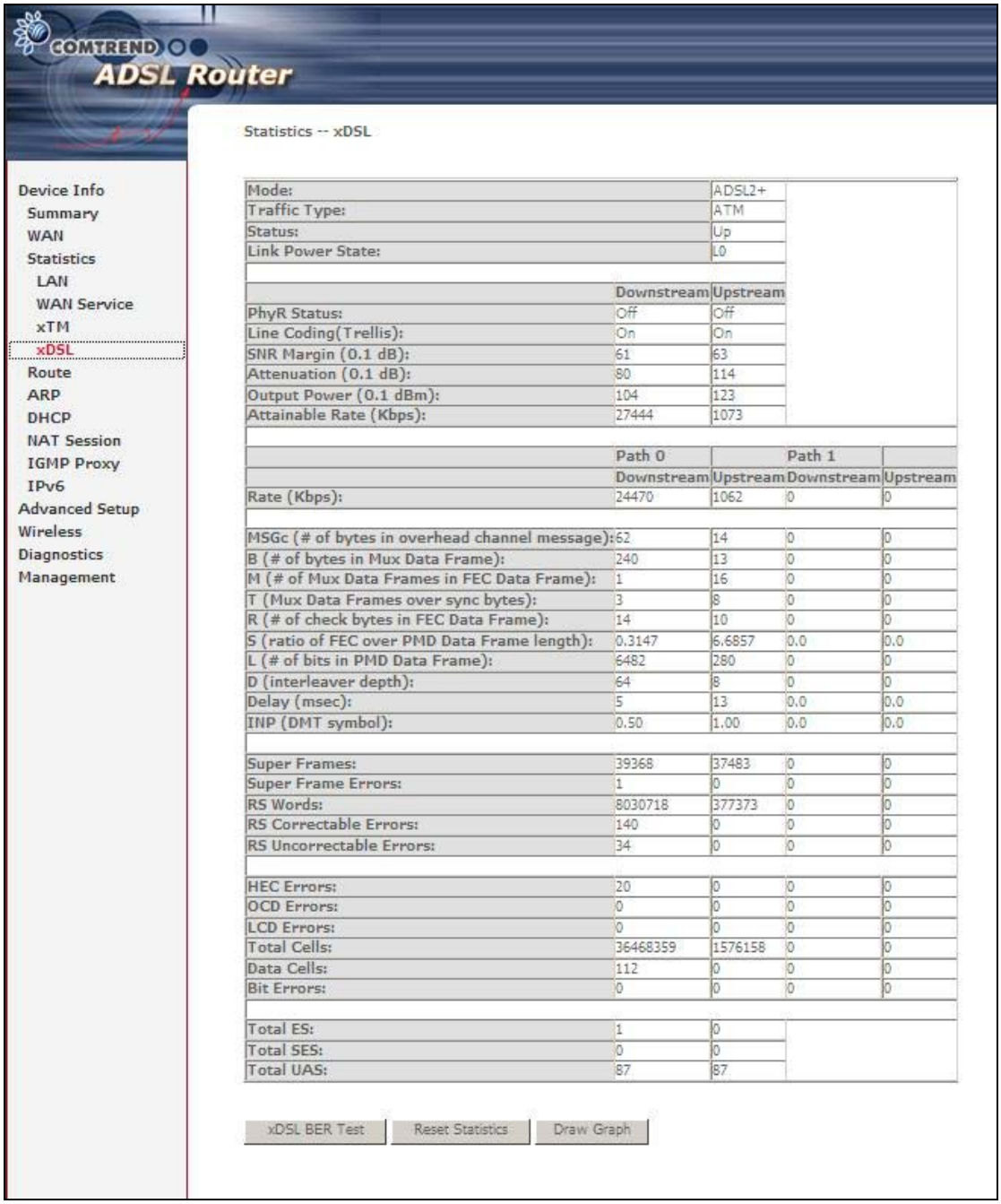
ATM Interface Statistics

Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of octets received over the interface
Out Octets	Number of octets transmitted over the interface
In Packets	Number of packets received over the interface
Out Packets	Number of packets transmitted over the interface
In OAM Cells	Number of OAM Cells received over the interface
Out OAM Cells	Number of OAM Cells transmitted over the interface
In ASM Cells	Number of ASM Cells received over the interface
Out ASM Cells	Number of ASM Cells transmitted over the interface
In Packet Errors	Number of packets in Error
In Cell Errors	Number of cells in Error.

4.2.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type.

ADSL



Mode:		ADSL2+
Traffic Type:		ATM
Status:		Up
Link Power State:		L0

	Downstream	Upstream
PhyR Status:	Off	Off
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	61	63
Attenuation (0.1 dB):	80	114
Output Power (0.1 dBm):	104	123
Attainable Rate (Kbps):	27444	1073

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	24470	1062	0	0
MSGc (# of bytes in overhead channel message):	62	14	0	0
B (# of bytes in Mux Data Frame):	240	13	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	16	0	0
T (Mux Data Frames over sync bytes):	3	8	0	0
R (# of check bytes in FEC Data Frame):	14	10	0	0
S (ratio of FEC over PMD Data Frame length):	0.3147	6.6857	0.0	0.0
L (# of bits in PMD Data Frame):	6482	280	0	0
D (interleaver depth):	64	8	0	0
Delay (msec):	5	13	0.0	0.0
INP (DMT symbol):	0.50	1.00	0.0	0.0
Super Frames:	39368	37483	0	0
Super Frame Errors:	1	0	0	0
RS Words:	8030718	377373	0	0
RS Correctable Errors:	140	0	0	0
RS Uncorrectable Errors:	34	0	0	0
HEC Errors:	20	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	36468359	1576158	0	0
Data Cells:	112	0	0	0
Bit Errors:	0	0	0	0
Total ES:	1	0		
Total SES:	0	0		
Total UAS:	87	87		

Click the **Reset Statistics** button to refresh this screen.

Field	Description
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+,
Traffic Type	Channel type Interleave or Fast

Field	Description
Status	Lists the status of the DSL link
Link Power State	Link output power state.
Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rates downstream/upstream

In ADSL2+ mode, the following section is inserted.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Mux Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)
INP	DMT symbol

In G.DMT mode, the following section is inserted.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

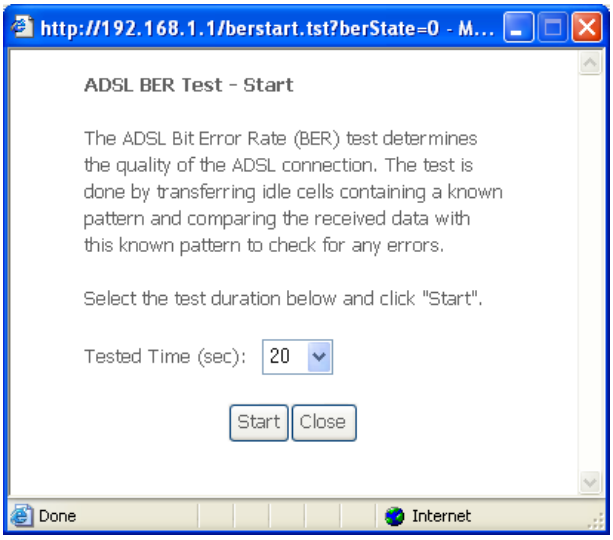
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)

Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

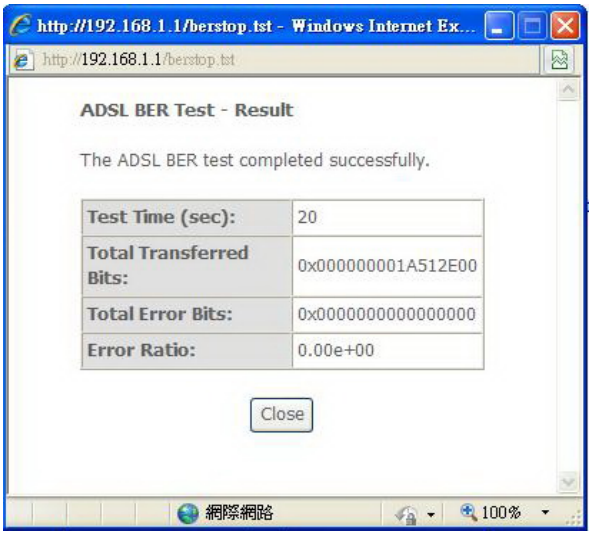
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

xDSL BER TEST

Click **xDSL BER Test** on the xDSL Statistics screen to test the Bit Error Rate (BER). A small pop-up window will open after the button is pressed, as shown below.

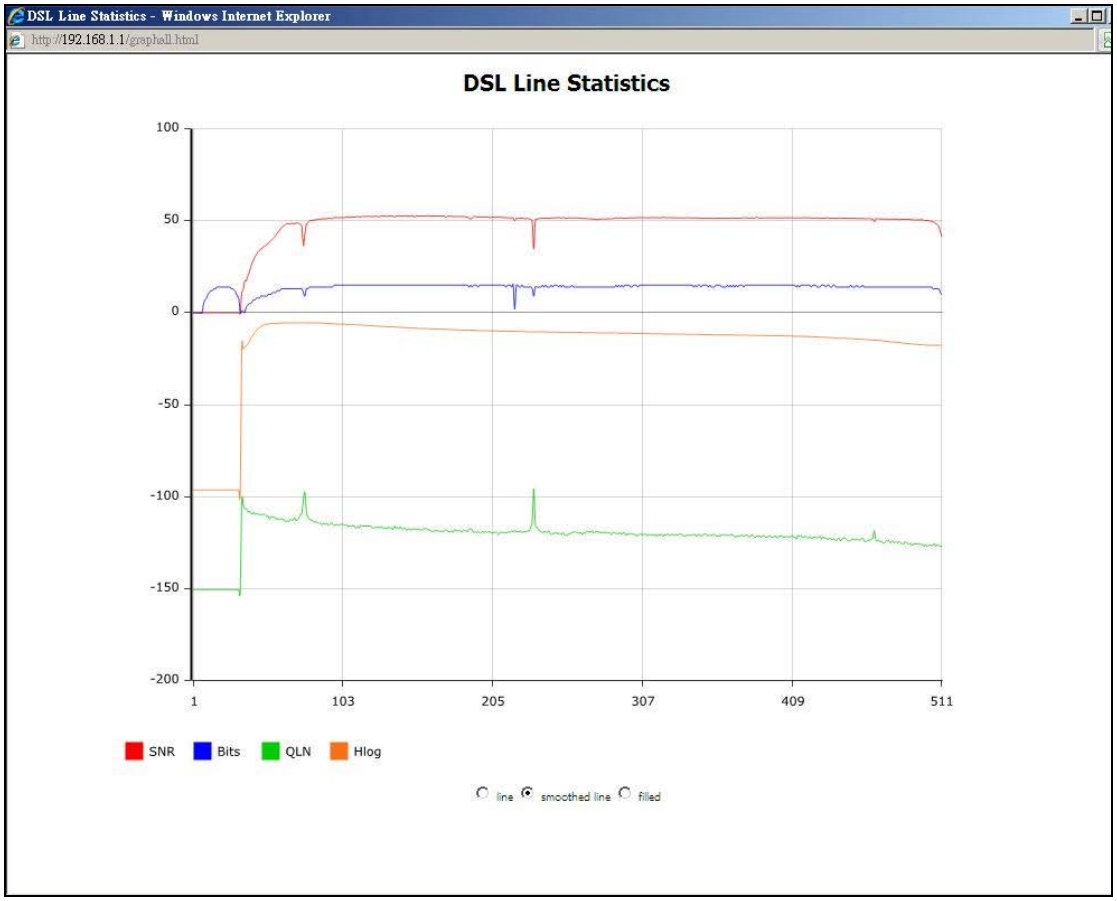

http://192.168.1.1/berstart.tst?berState=0 - M...
ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close
Done
Internet

Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



xDSL GRAPH

Click **Draw Graph** on the xDSL Statistics screen and a pop-up window will display the xDSL bits per tone status, SNR, QLN and Hlog of the current xDSL connection, as shown below.



4.3 Route

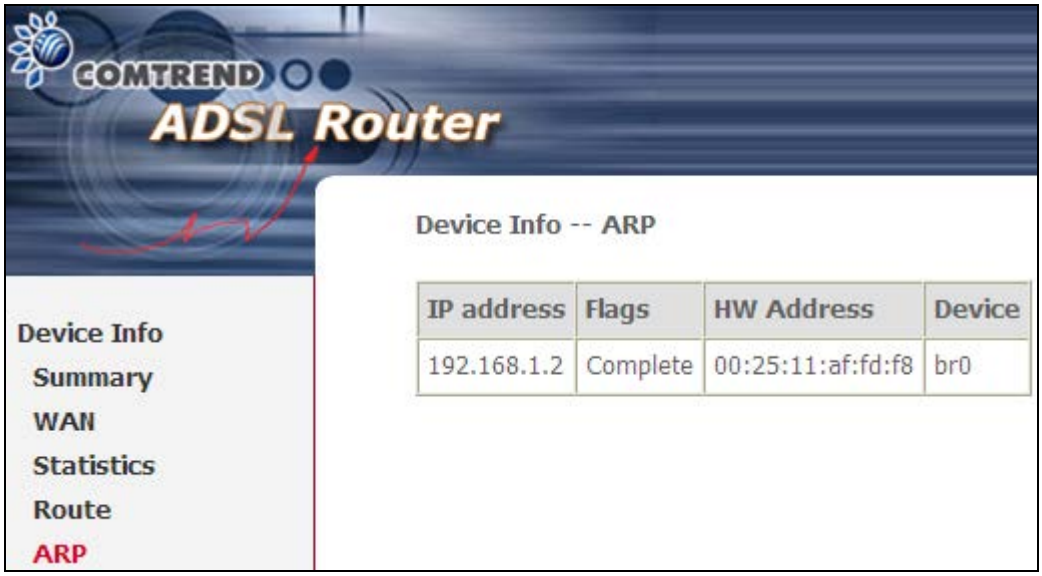
Choose **Route** to display the routes that the AR-5389 has found.

COMTREND
ADSL Router
Device Info -- Route
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).
Device Info
Summary
WAN
Statistics
Route
Destination Gateway Subnet Mask Flag Metric Service Interface
192.168.1.0 0.0.0.0 255.255.255.0 U 0 br0

Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

4.4 ARP

Click **ARP** to display the ARP information.

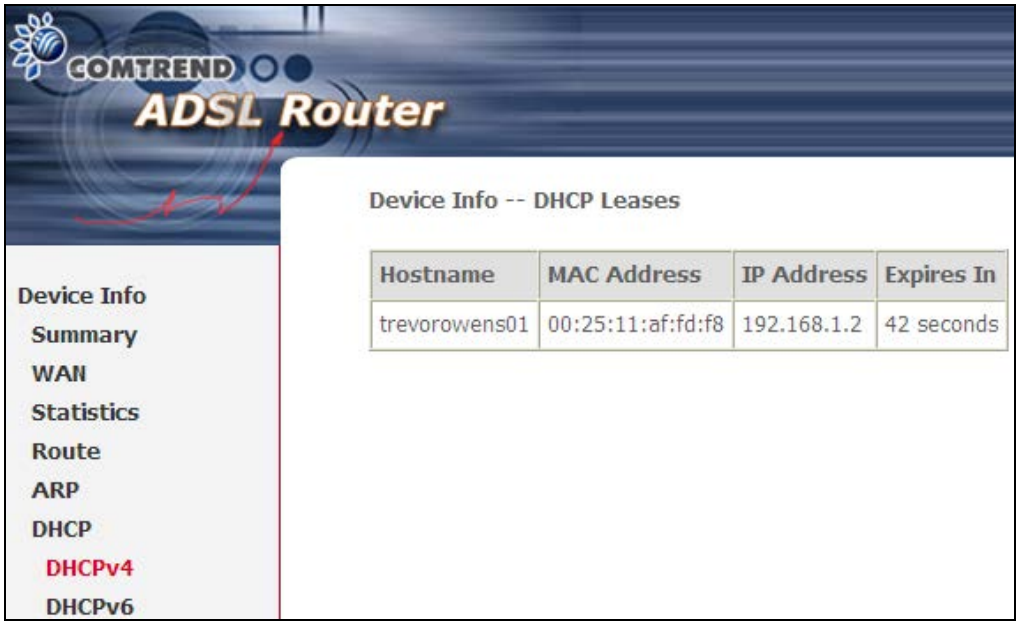


Field	Description
IP address	Shows IP address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

4.5 DHCP

4.5.1 DHCPv4

Click **DHCPv4** to display all DHCPv4 Leases.



Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

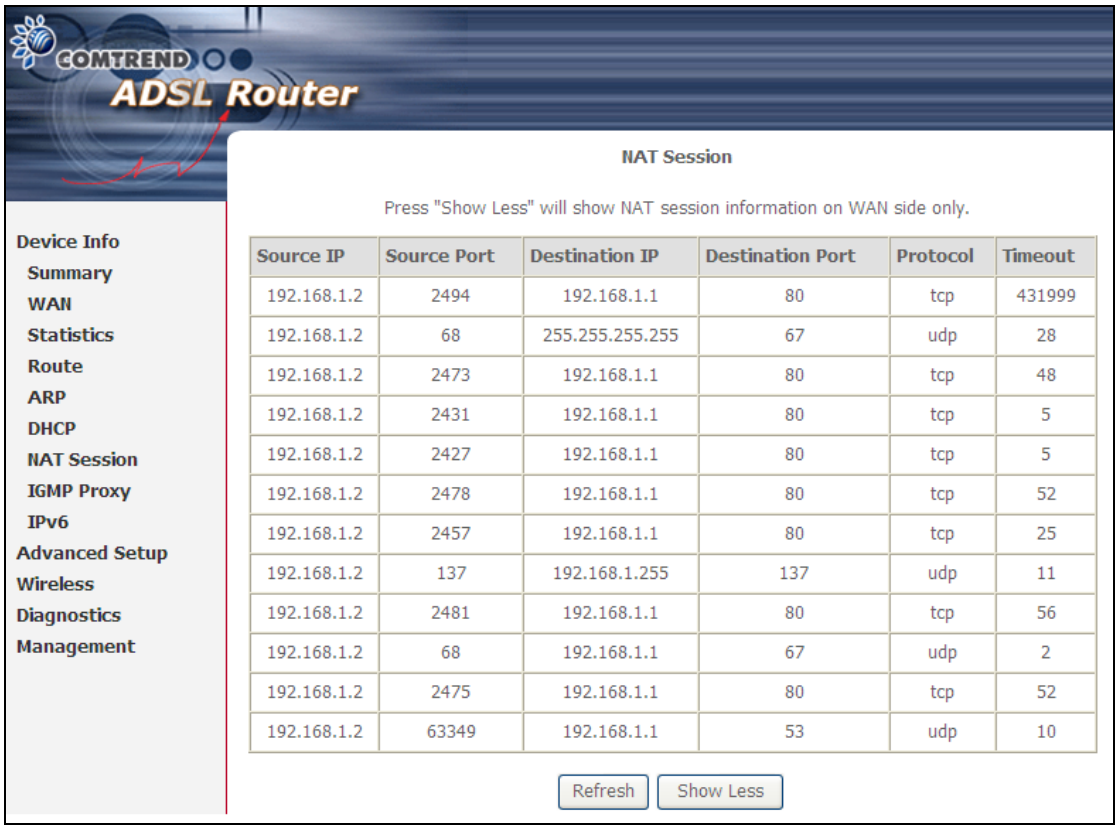
4.5.2 DHCPv6

Click **DHCPv6** to display all DHCPv6 Leases.

Field	Description
IPv6 Address	Shows IP address of device/host/PC
MAC Address	Shows the Ethernet MAC address of the device/host/PC
Duration	Shows leased time in hours
Expires In	Shows how much time is left for each DHCP Lease

4.6 NAT Session

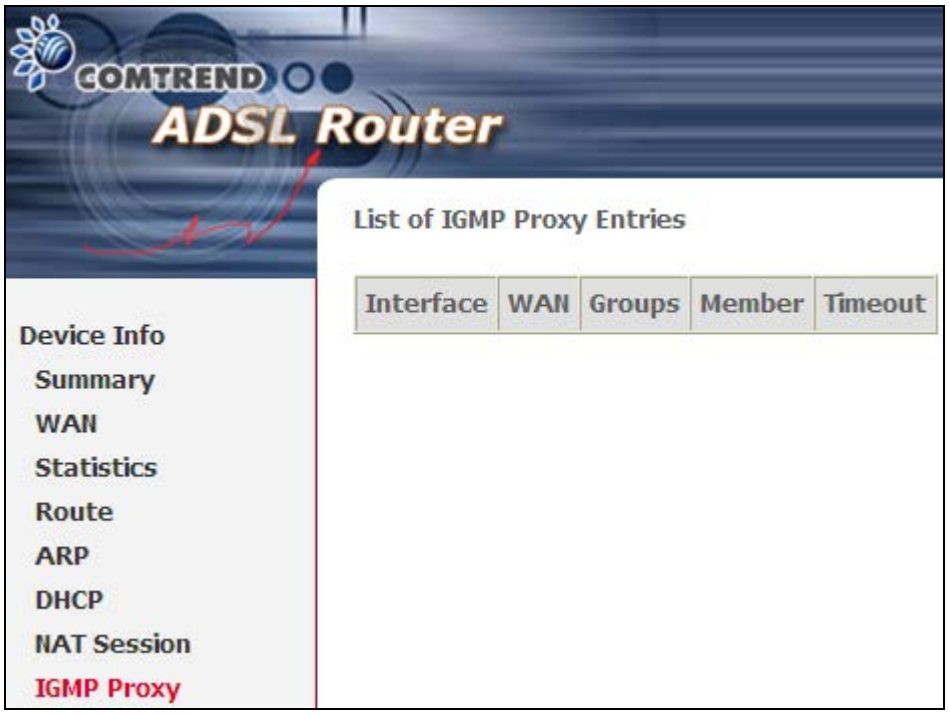
Press "Show All" to show all NAT session information.


COMTREND
ADSL Router
Device Info
Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6
Advanced Setup
Wireless
Diagnostics
Management
NAT Session
Press "Show Less" will show NAT session information on WAN side only.
Source IP | Source Port | Destination IP | Destination Port | Protocol | Timeout
192.168.1.2 | 2494 | 192.168.1.1 | 80 | tcp | 431999
192.168.1.2 | 68 | 255.255.255.255 | 67 | udp | 28
192.168.1.2 | 2473 | 192.168.1.1 | 80 | tcp | 48
192.168.1.2 | 2431 | 192.168.1.1 | 80 | tcp | 5
192.168.1.2 | 2427 | 192.168.1.1 | 80 | tcp | 5
192.168.1.2 | 2478 | 192.168.1.1 | 80 | tcp | 52
192.168.1.2 | 2457 | 192.168.1.1 | 80 | tcp | 25
192.168.1.2 | 137 | 192.168.1.255 | 137 | udp | 11
192.168.1.2 | 2481 | 192.168.1.1 | 80 | tcp | 56
192.168.1.2 | 68 | 192.168.1.1 | 67 | udp | 2
192.168.1.2 | 2475 | 192.168.1.1 | 80 | tcp | 52
192.168.1.2 | 63349 | 192.168.1.1 | 53 | udp | 10
Refresh
Show Less

Pressing "Show Less" will show NAT session information on the WAN side only.

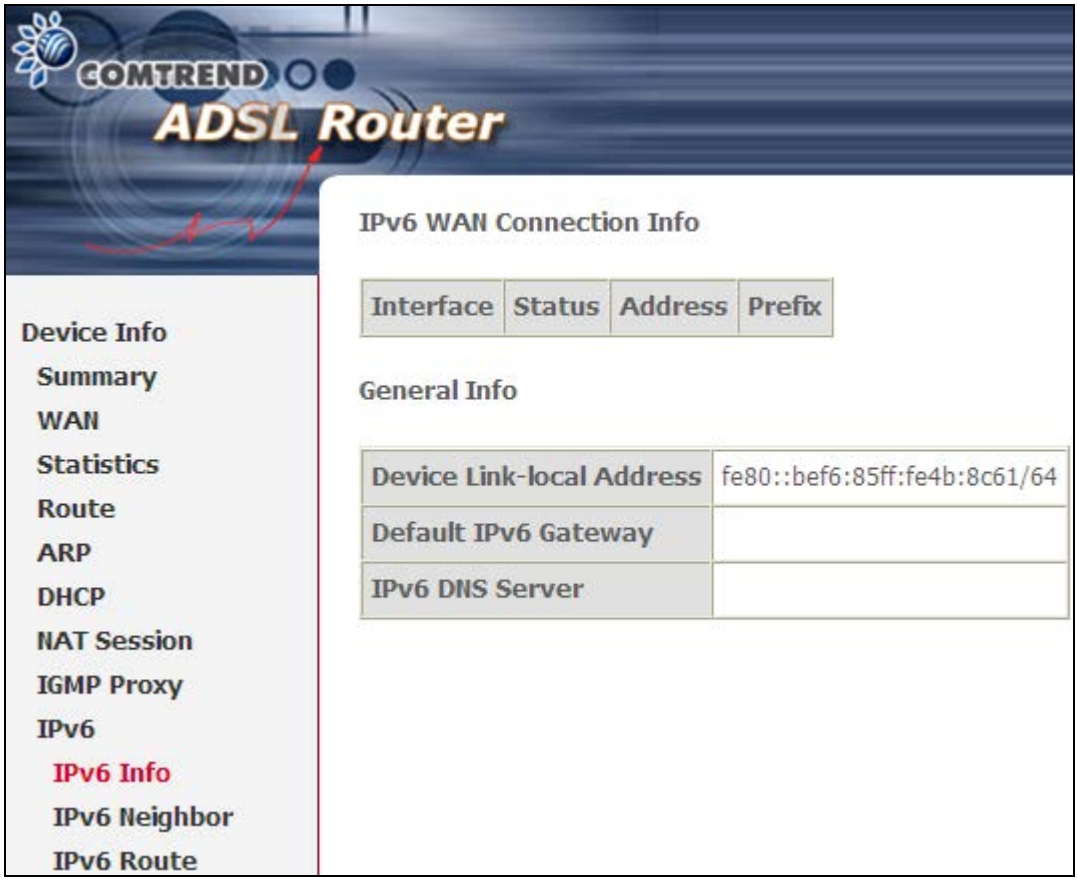
4.7 IGMP Proxy

Displays a list of IGMP Proxy entries.



4.8 IPv6

4.8.1 IPv6 Info



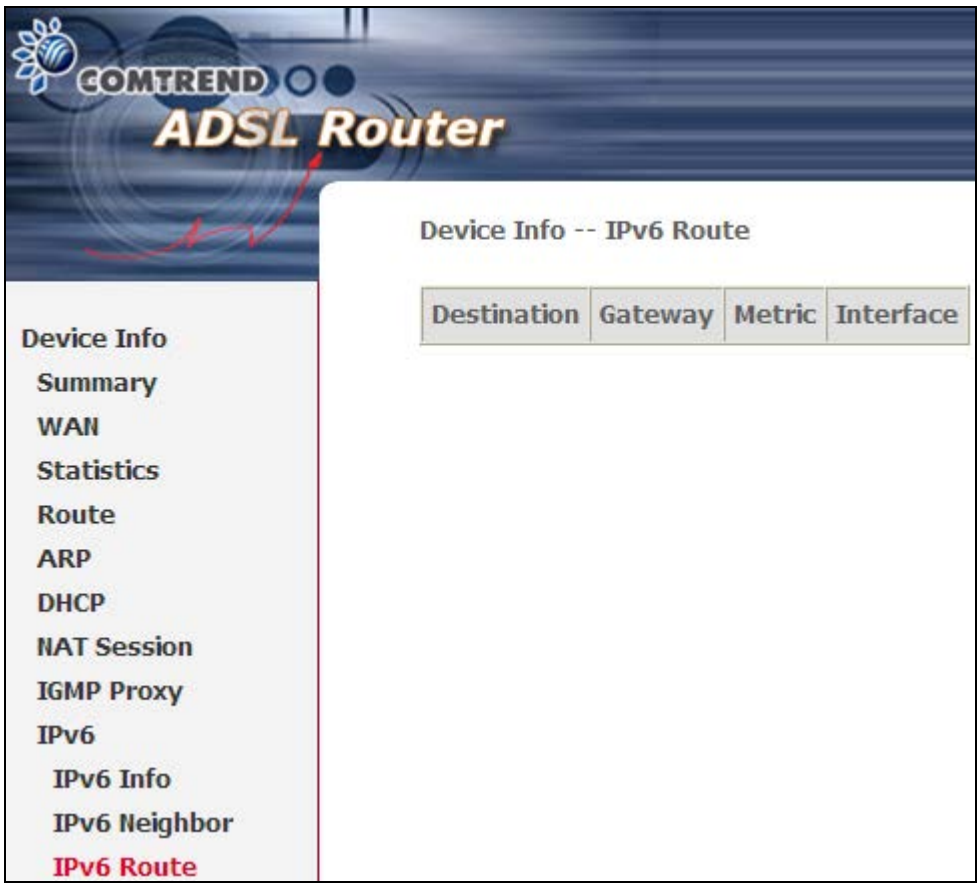
Field	Description
Interface	WAN interface with IPv6 enabled
Status	Connection status of the WAN interface
Address	IPv6 Address of the WAN interface
Prefix	Prefix received/configured on the WAN interface
Device Link-local Address	The CPE's LAN Address
Default IPv6 Gateway	The default WAN IPv6 gateway
IPv6 DNS Server	The IPv6 DNS servers received from the WAN interface / configured manually

4.8.2 IPv6 Neighbor

Provides a list of IPv6 devices found in the network.

Field	Description
IPv6 Address	Ipv6 address of the device(s) found
Flags	Status of the neighbor device
HW Address	MAC address of the neighbor device
Device	Interface from which the device is located

4.8.3 IPv6 Route



Field	Description
Destination	Destination IP Address
Gateway	Gateway address used for destination IP
Metric	Metric specified for gateway
Interface	Interface used for destination IP

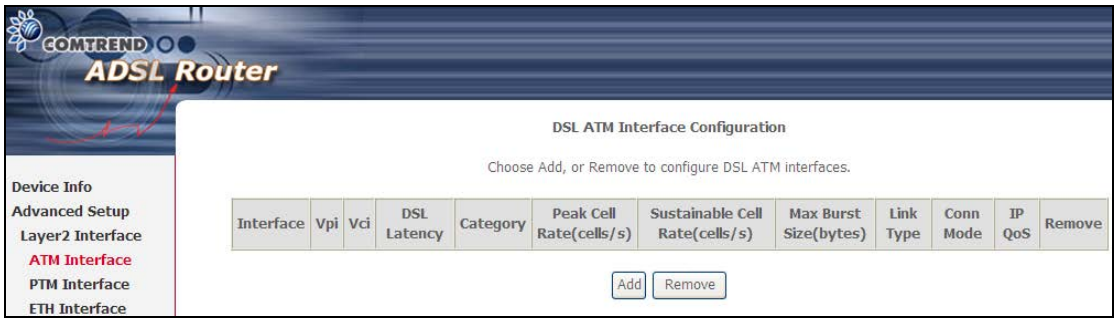
Chapter 5 Advanced Setup

5.1 Layer 2 Interface

The ATM interface screen is described here.

5.1.1 ATM Interface

Add or remove ATM interface connections here.



Click **Add** to create a new ATM interface (see Appendix E - Connection Setup).

NOTE:	Up to 16 ATM interfaces can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **Remove**.

5.1.2 PTM Interface

Add or remove PTM interface connections here.

Click **Add** to create a new connection (see Appendix E - Connection Setup). To remove a connection, select its Remove column radio button and click **Remove**.

5.1.3 ETH Interface

This screen displays the Ethernet WAN Interface configuration.

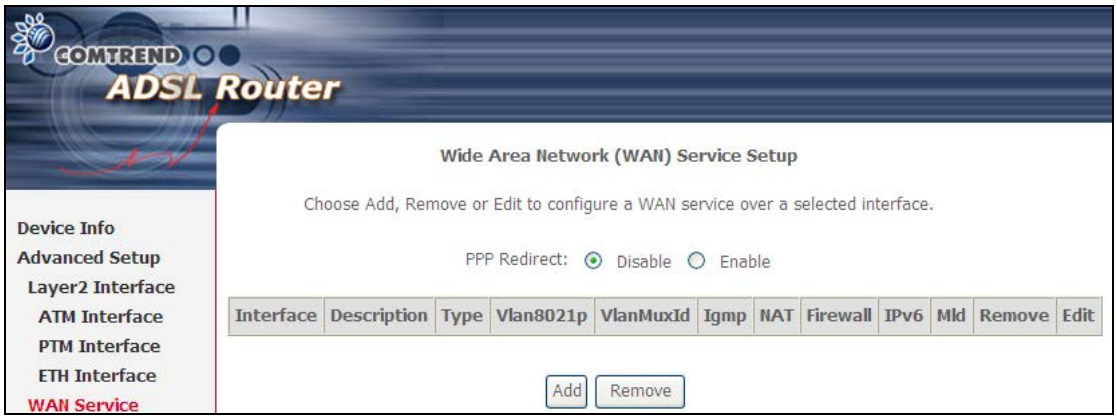
Click **Add** to create a new connection (see Appendix E - Connection Setup).

NOTE: One Ethernet WAN interface can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **remove.**

5.2 WAN Service

This screen allows for the configuration of WAN interfaces.



Click the **Add** button to create a new connection. For connections on ATM or ETH WAN interfaces see Appendix E - Connection Setup.

NOTE:	In Default Mode, up to 16 WAN connections can be configured; while VLAN Mux Connection Mode supports up to 16 WAN connections.

To remove a connection, select its Remove column radio button and click **Remove.**

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD	Shows Multicast Listener Discovery (MLD) status
Remove	Select interfaces to remove

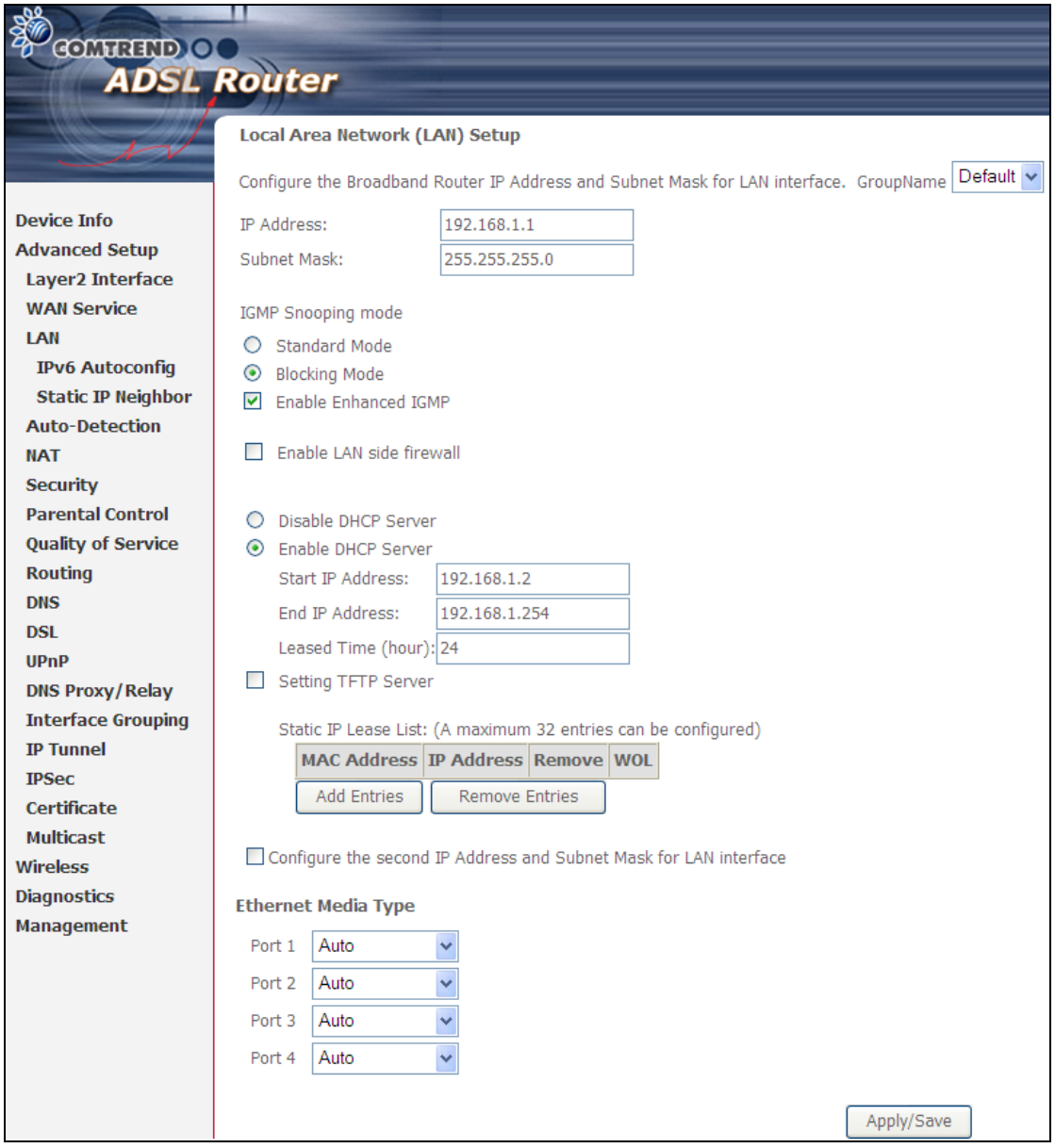
To remove a connection, select its Remove column radio button and click **Remove.**

To **Add** a new WAN connection, click the **Add** button and follow the instructions.

NOTE:	Up to 16 PVC profiles can be configured and saved in flash memory.

5.3 LAN

Configure the LAN interface settings and then click **Apply / Save**.



Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable IGMP Snooping: Enable by ticking the checkbox ☑.

Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

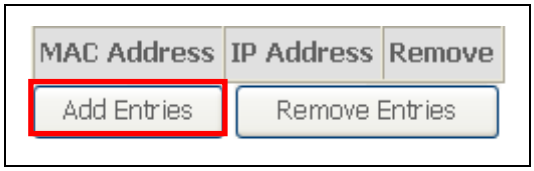
Enable Enhanced IGMP: Enable by ticking the checkbox ☑. IGMP packets between LAN ports will be blocked.

Enable LAN side firewall: Enable by ticking the checkbox ☑.

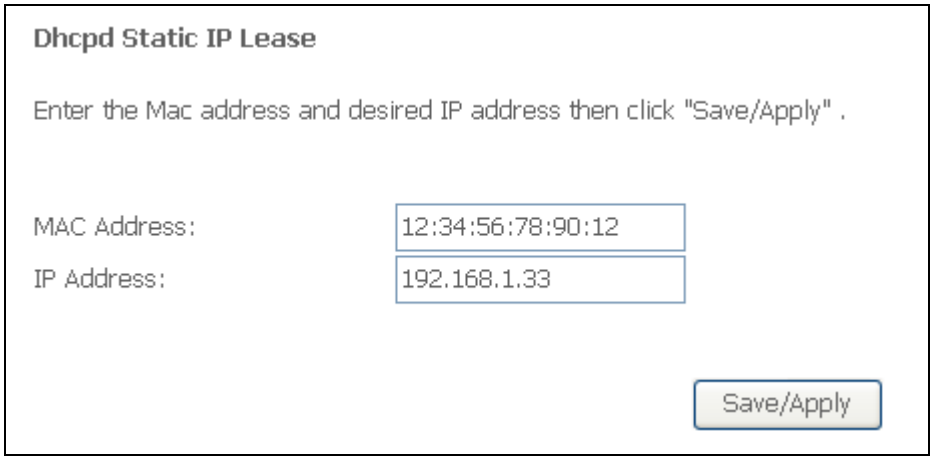
DHCP Server: To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Setting TFTP Server: Enable by ticking the checkbox ☑. Then, input the TFTP server address or an IP address.

Static IP Lease List: A maximum of 32 entries can be configured.



To add an entry, enter MAC address and Static IP and then click **Save / Apply**.

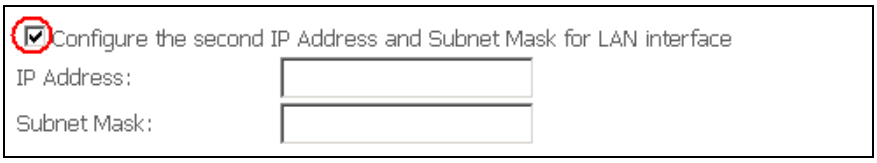


To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.

DHCP Server Relay: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. ***This option is hidden if NAT is enabled or when the router is configured with only one Bridge PVC.***

2ND LAN INTERFACE

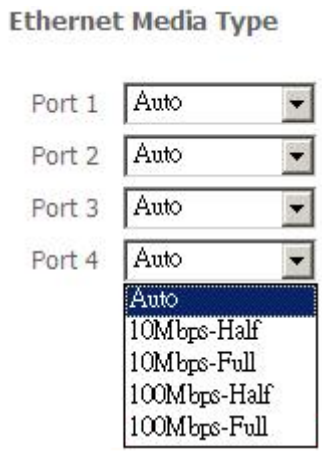
To configure a secondary IP address, tick the checkbox ☑ outlined (in RED) below.



IP Address: Enter the secondary IP address for the LAN port.
Subnet Mask: Enter the secondary subnet mask for the LAN port.

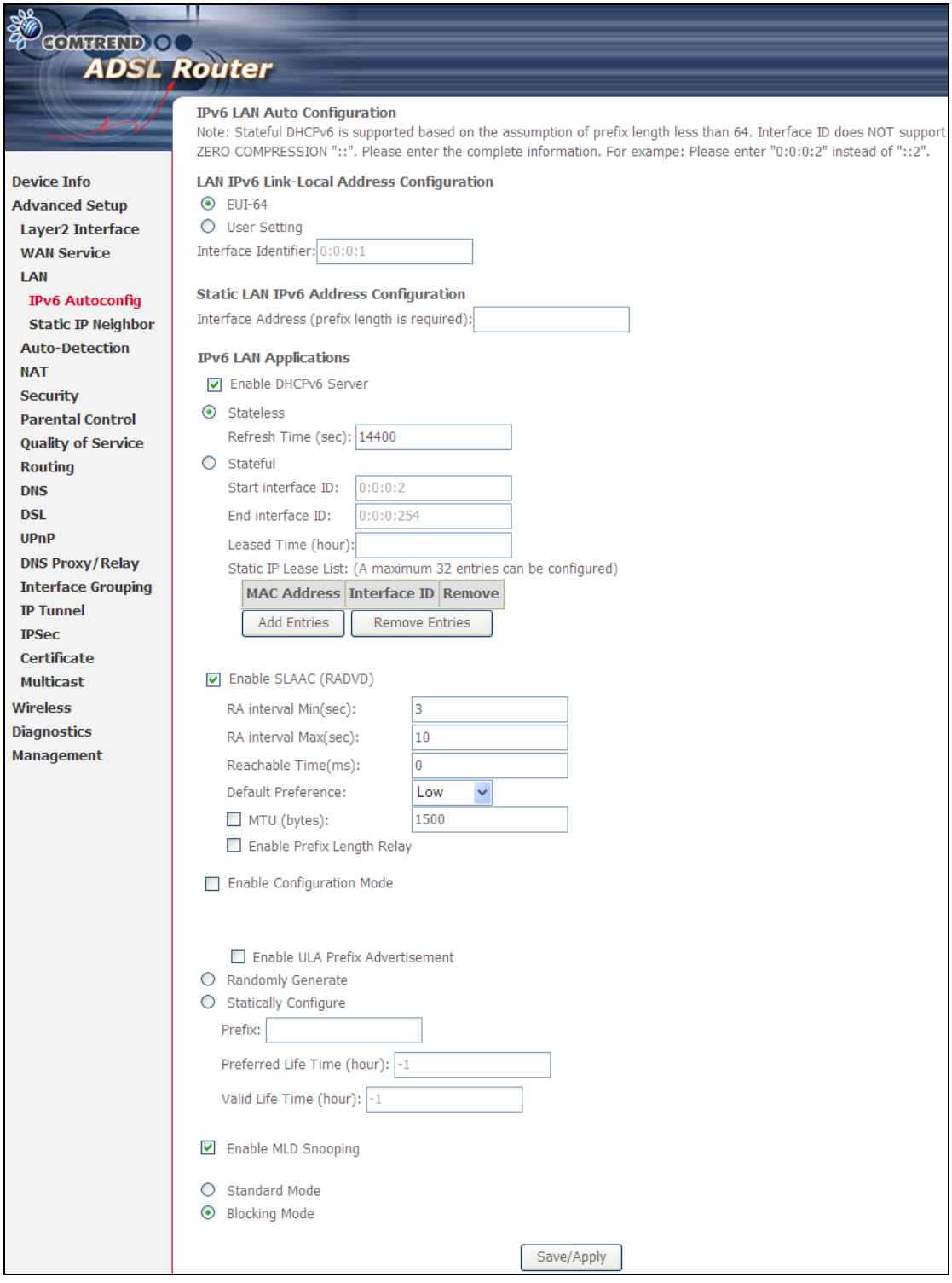
Ethernet Media Type:

Configure auto negotiation, or enforce selected speed and duplex mode for each Ethernet port.



5.3.1 LAN IPv6 Autoconfig

Configure the LAN interface settings and then click **Save / Apply**.



Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

Heading	Description
EUI-64	Use EUI-64 algorithm to calculate link-local address from MAC address
User Setting	Use the Interface Identifier field to define a link-local address

Static LAN IPv6 Address Configuration

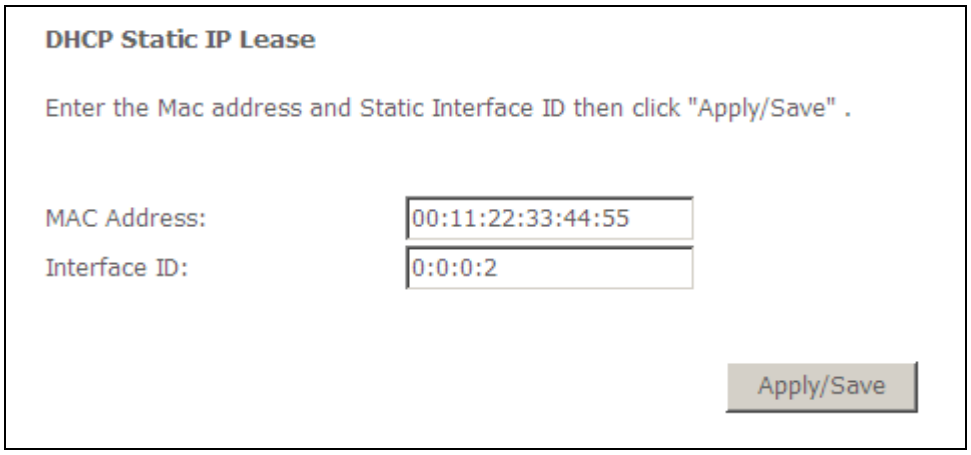
Heading	Description
Interface Address (prefix length is required):	Configure static LAN IPv6 address and subnet prefix length

IPv6 LAN Applications

Heading	Description
Stateless	Use stateless configuration
Refresh Time (sec):	The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6
Stateful	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to dhcpv6 client
End interface ID:	End of interface ID to be assigned to dhcpv6 client
Leased Time (hour):	Lease time for dhcpv6 client to use the assigned IP address

Static IP Lease List: A maximum of 32 entries can be configured.

To add an entry, enter MAC address and Static IP and then click **Apply/Save**.



To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.

Heading	Description
Enable RADVD	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable Configuration Mode	Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure Prefix	Specify the prefix to be used
Statically Configure	The prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix
Valid Life Time (hour)	The valid life time for this prefix
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports

5.3.2 Static IP Neighbor

Click the Add button to display the following.

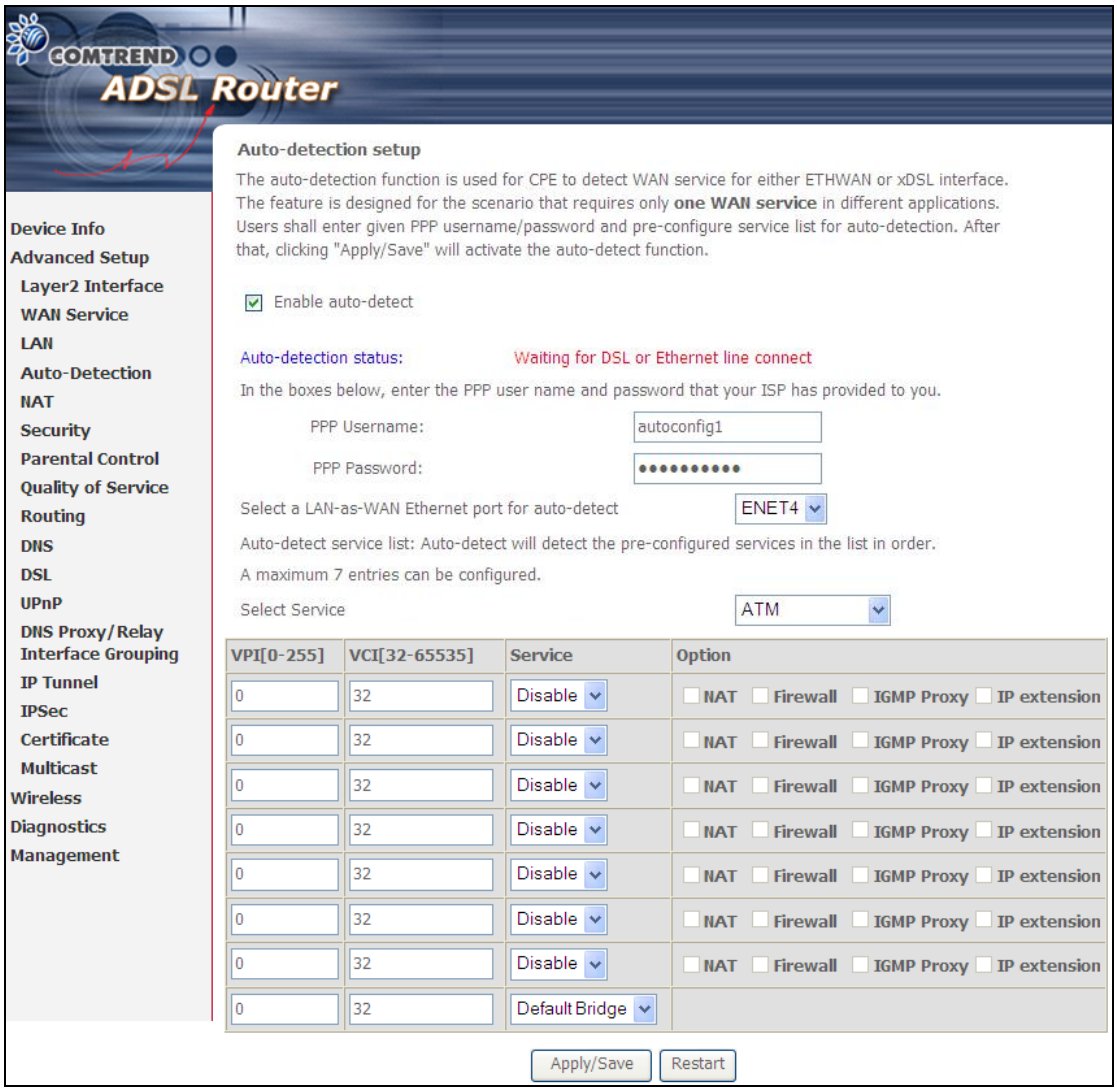
Heading	Description
IP Version	The IP version used for the neighbor device
IP Address	Define the IP Address for the neighbor device
MAC Address	The MAC Address of the neighbor device
Associated Interface	The interface where the neighbor device is located

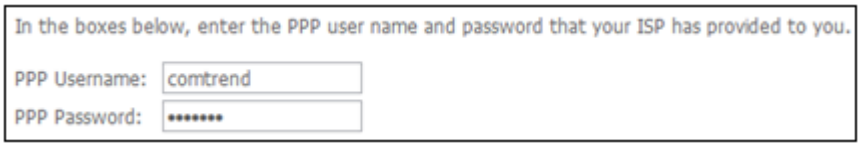
5.4 Auto-Detection

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications.

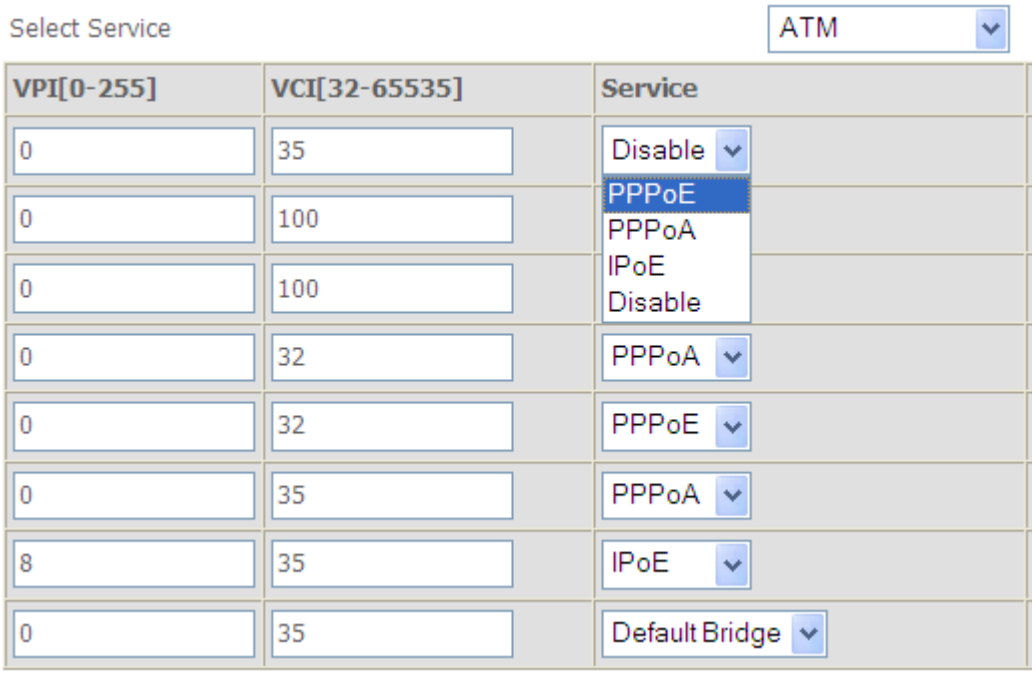
COMTREND
ADSL Router
Auto-detection setup
The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only one WAN service in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.
Enable auto-detect
Apply/Save
Restart
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT

The Auto Detection page simply provides a checkbox allowing users to enable or disable the feature. Check the checkbox to display the following configuration options.

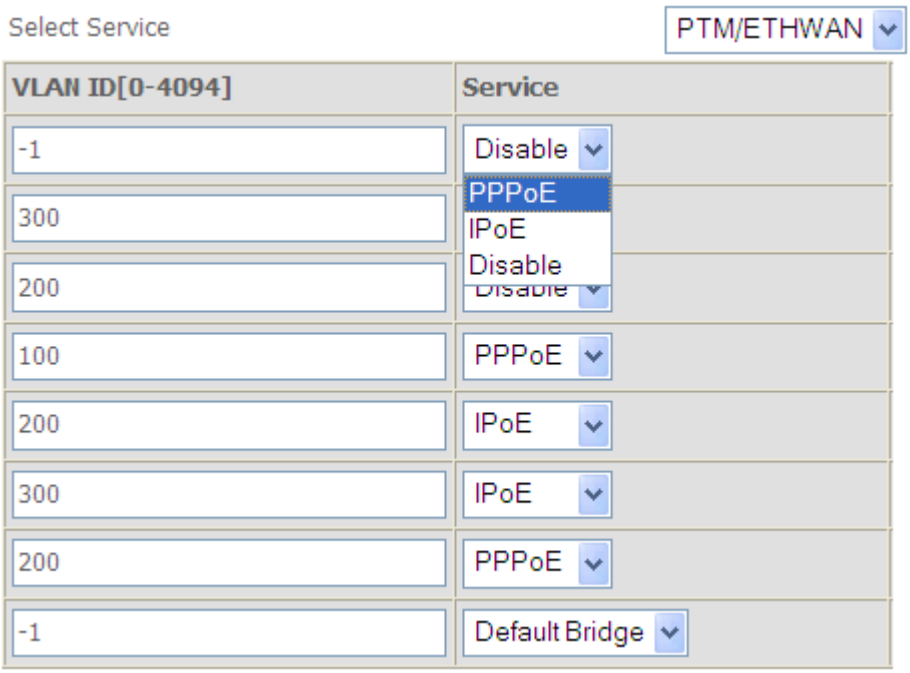

COMTREND
ADSL Router
Auto-detection setup
The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only one WAN service in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.
Enable auto-detect
Auto-detection status: Waiting for DSL or Ethernet line connect
In the boxes below, enter the PPP user name and password that your ISP has provided to you.
PPP Username: autoconfig1
PPP Password:
Select a LAN-as-WAN Ethernet port for auto-detect ENET4
Auto-detect service list: Auto-detect will detect the pre-configured services in the list in order.
A maximum 7 entries can be configured.
Select Service ATM
VPI[0-255] VCI[32-65535] Service Option
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Disable NAT Firewall IGMP Proxy IP extension
0 32 Default Bridge
Apply/Save
Restart
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy/Relay
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management


In the boxes below, enter the PPP user name and password that your ISP has provided to you.
PPP Username: comtrend
PPP Password: •••••••

Enter the PPP username/password given by your service provider for PPP service detection.



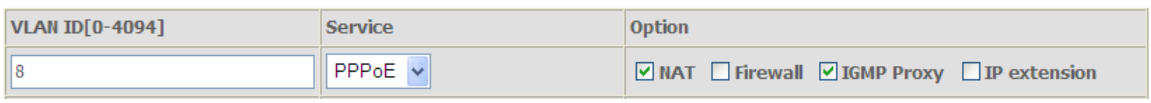
WAN services list for ATM mode: A maximum of 7 WAN services with corresponding PVC are required to be configured for ADSL ATM mode. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of those services to meet their own requirement and also reduce the detection cycle.



WAN services list for PTM mode: A maximum of 7 WAN services with corresponding VLAN ID (-1 indicates no VLAN ID is required for the service) are required to be configured for ADSL/VDSL PTM mode and ETHWAN. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of the services to meet their own requirement and also reduce the detection cycle.

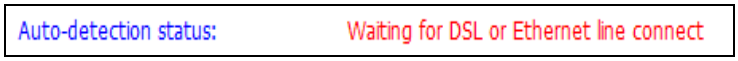
Click "Apply/Save" to activate the auto-detect function.

Options for each WAN service: These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

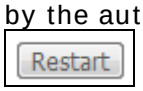


Auto Detection status and Restart

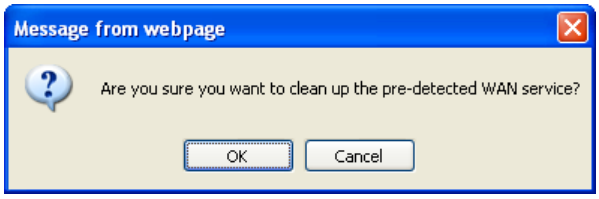
The Auto-detection status is used to display the real time status of the Auto-detection feature.



The **Restart** button is used to detect all the WAN services that are either detected by the auto-detection feature or configured manually by users.



The following window will pop up upon clicking the **Restart** button. Click the **OK** button to proceed.



Auto Detection notice

1) This feature will automatically detect one WAN service only. If customers require multiple WAN services, manual configuration is required.
2) If a physical ETHWAN port is detected, the Auto Detection for ETHWAN will be fixed on the physical ETHWAN port and cannot be configured for any LAN port; if the physical ETHWAN port is not detected, the Auto Detection for ETHWAN will be configured to the 4th LAN port by default and allows it to be configured for any LAN port as well.
3) For cases in which both the DSL port and ETHWAN port are plugged in at the same time, the DSL WAN will have priority over ETHWAN. For example, the ETHWAN port is plugged in with a WAN service detected automatically and then the DSL port is plugged in and linked up. The Auto Detection feature will clear the WAN service for ETHWAN and re-detect the WAN service for DSL port.
4) If none of the pre-configured services are detected, a Bridge service will be created.

5.5 NAT

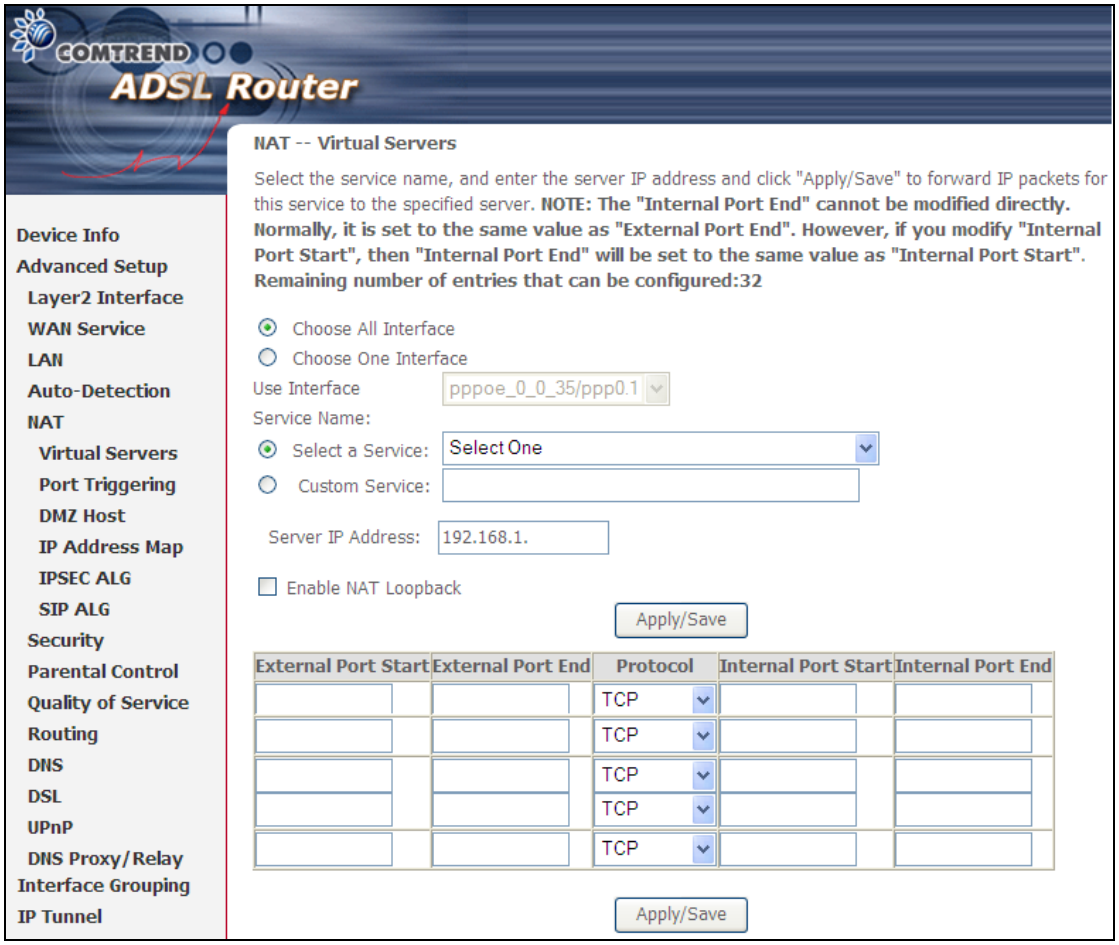
To display this option, NAT must be enabled in at least one PVC shown on the Chapter 5 Advanced Setup. *NAT is not an available option in Bridge mode*.

5.5.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
A maximum of 32 entries can be configured.

COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
NAT -- Virtual Servers Setup
Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.
Add
Remove
Server Name
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
Server IP Address
WAN Interface
NAT Loopback
Remove

To add a Virtual Server, click **Add**. The following will be displayed.



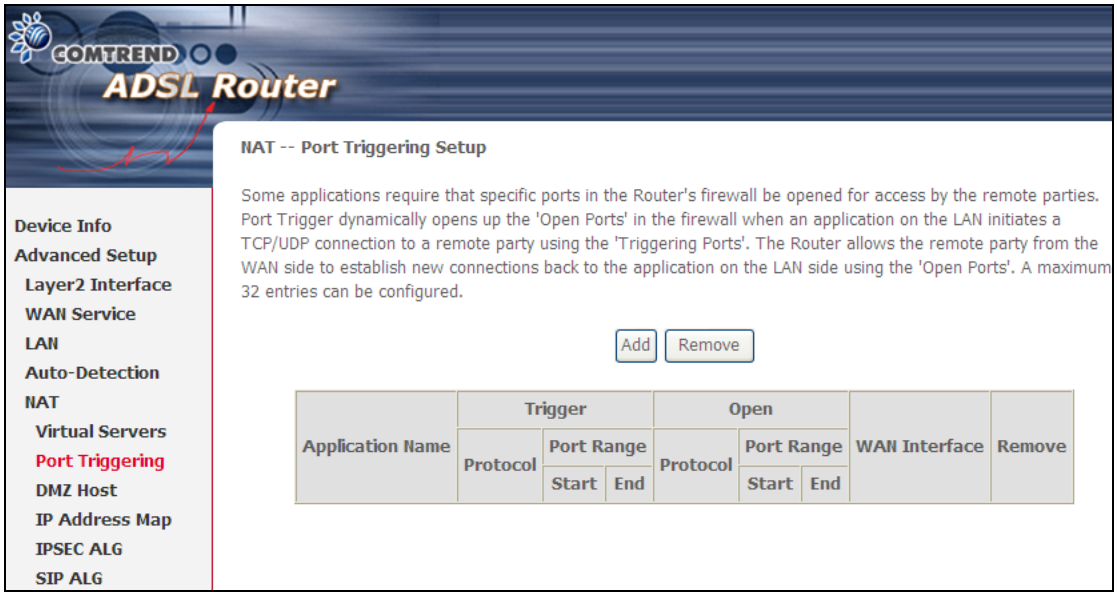
Consult the table below for field and header descriptions.

Field/Header	Description
Choose All Interface	Virtual server rules will be created for all WAN interfaces.
Choose One Interface	Select a WAN Interface from Use Interface list to apply the virtual server rule.
Use Interface	Select a WAN interface from the drop-down box.
Select a Service **Or** Custom Service	User should select the service from the list. **Or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
Enable NAT Loopback	Allows local machines to access virtual server via WAN IP Address.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.

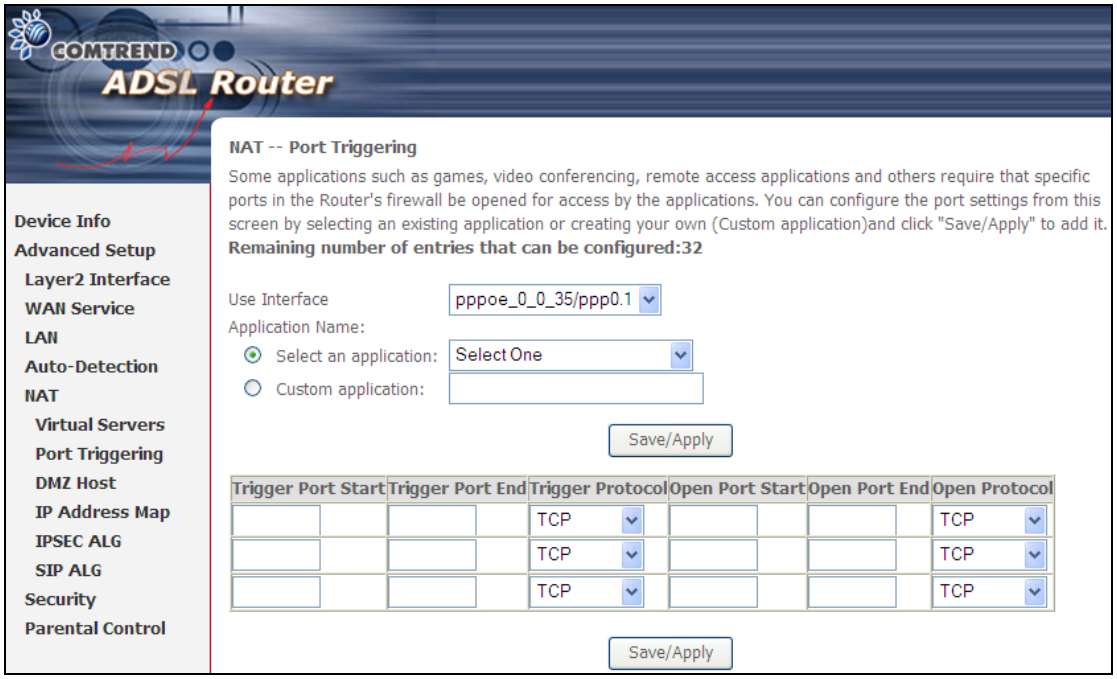
Field / Header	Description
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

5.5.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.


COMTREND
ADSL Router
NAT -- Port Triggering Setup
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.
Add
Remove
Application Name
Trigger
Protocol
Port Range
Start
End
Open
Protocol
Port Range
Start
End
WAN Interface
Remove
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG

To add a Trigger Port, click **Add**. The following will be displayed.

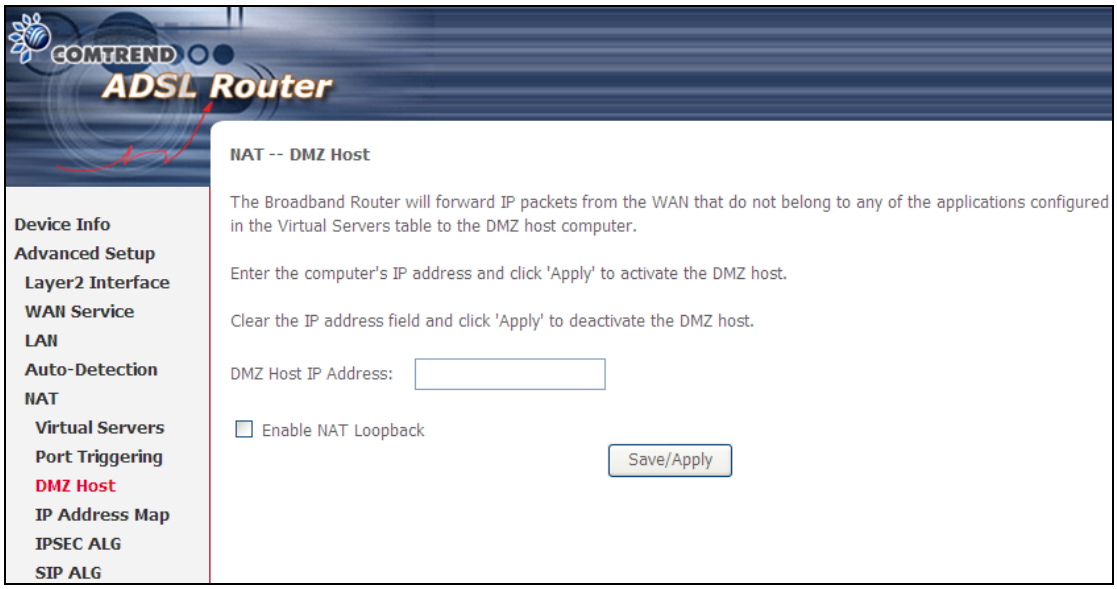


Consult the table below for field and header descriptions.

Field / Header	Description
Use Interface	Select a WAN interface from the drop-down box.
Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP, or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP, or UDP.

5.5.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
NAT -- DMZ Host
The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click 'Apply' to activate the DMZ host.
Clear the IP address field and click 'Apply' to deactivate the DMZ host.
DMZ Host IP Address:
Enable NAT Loopback
Save/Apply

To **Activate** the DMZ host, enter the DMZ host IP address and click **Save / Apply**.

To **Deactivate** the DMZ host, clear the IP address field and click **Save / Apply**.

Enable NAT loopback – Select to allow local machines to access the DMZ server via the WAN IP Address.

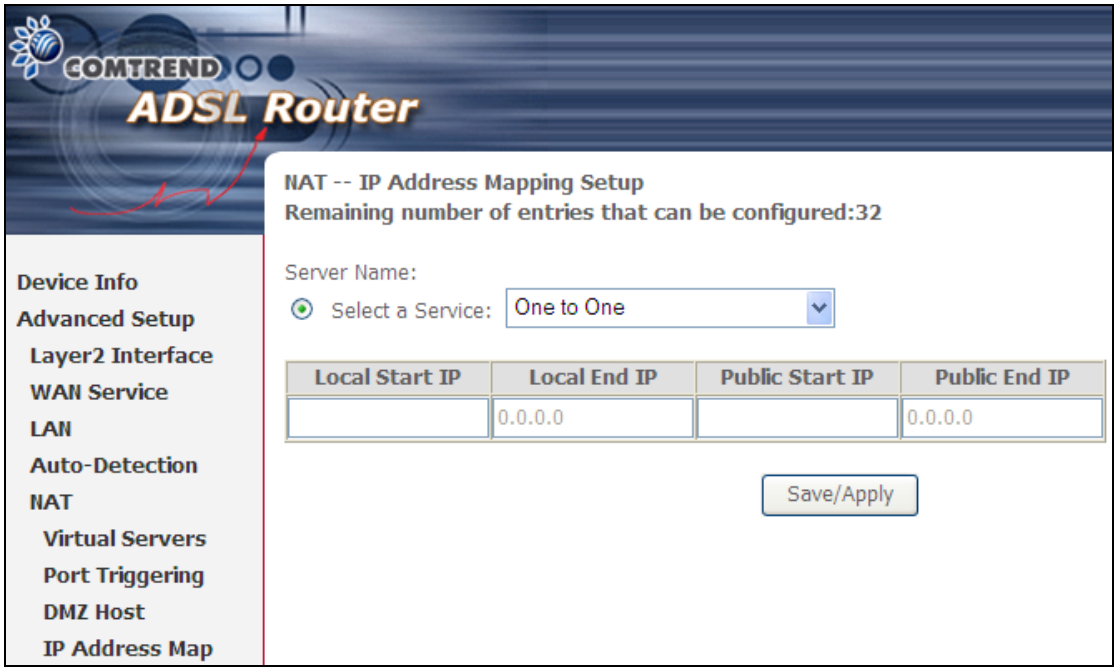
5.5.4 IP Address Map

Mapping Local IP (LAN IP) to some specified Public IP (WAN IP).

Consult the table below for field and header descriptions.

Field / Header	Description
Rule	The number of the rule
Type	Mapping type from local to public.
Local Start IP	The beginning of the local IP
Local End IP	The ending of the local IP
Public Start IP	The beginning of the public IP
Public End IP	The ending of the public IP
Remove	Remove this rule

Click the Add button to display the following screen.

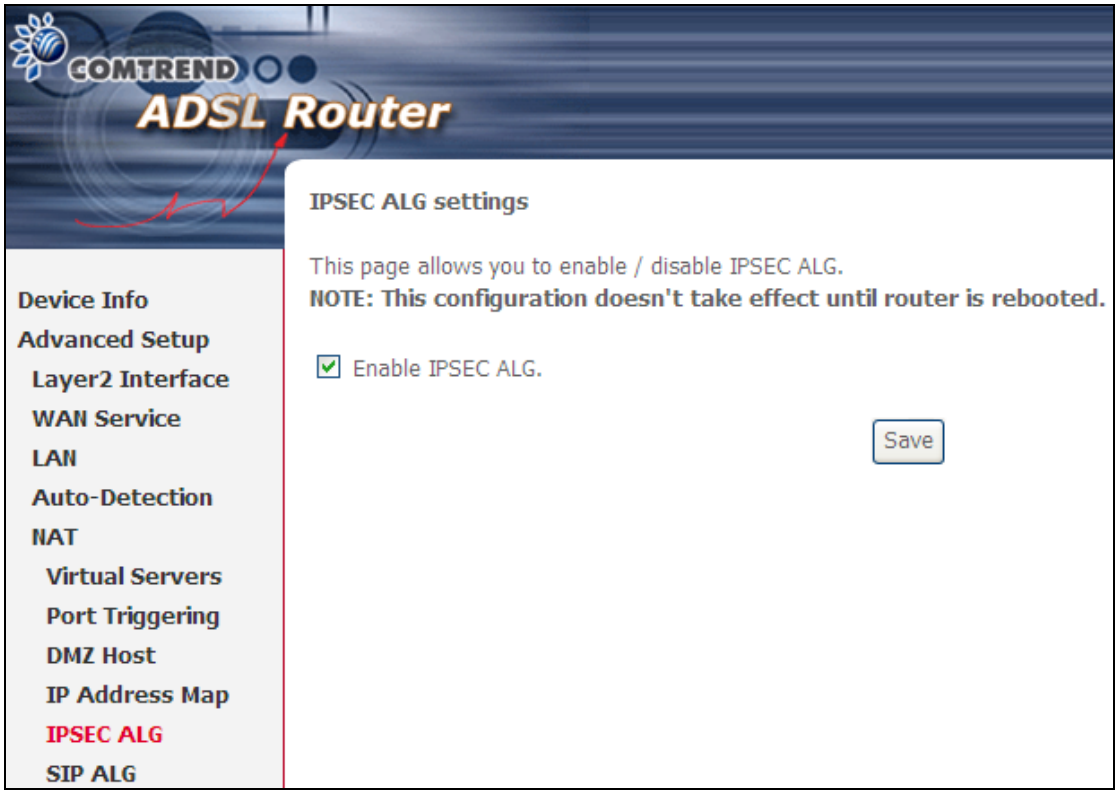


Select a Service, then click the **Save / Apply** button.

One to One: mapping one local IP to a specific public IP
Many to One: mapping a range of local IP to a specific public IP
Many to Many(Overload): mapping a range of local IP to a different range of public IP
Many to Many(No Overload): mapping a range of local IP to a same range of public IP

5.5.5 IPSEC ALG

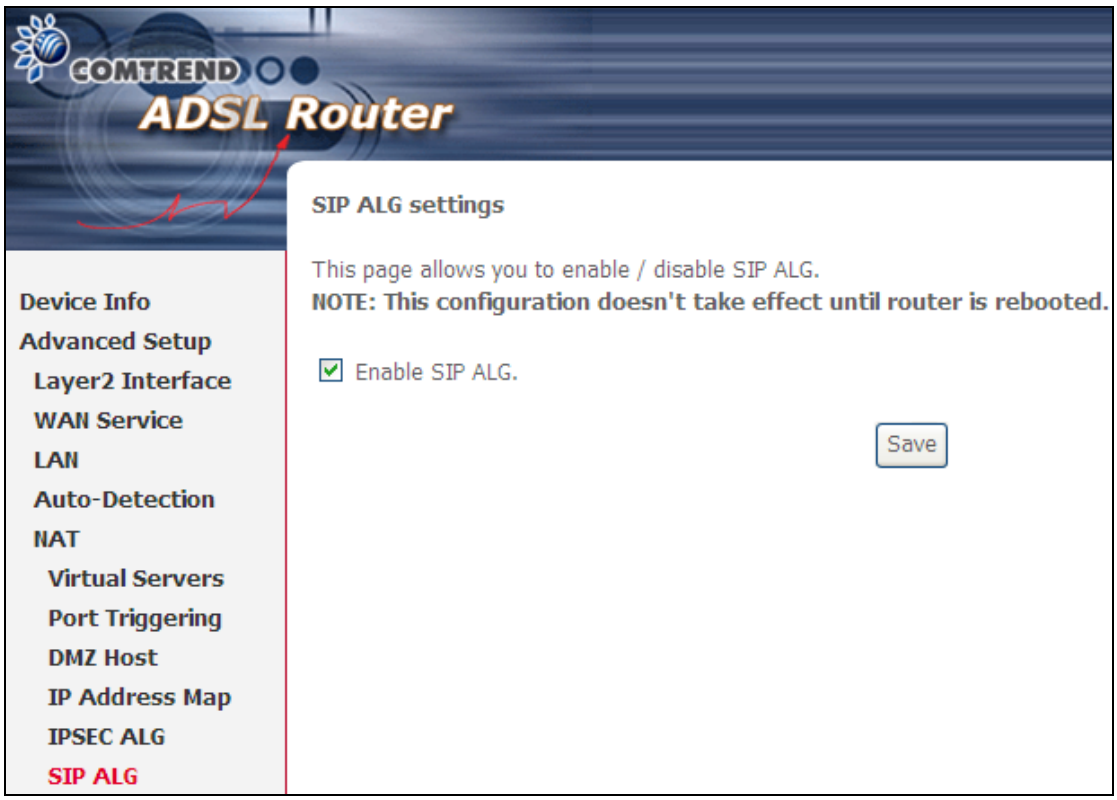
IPSEC ALG provides multiple VPN passthrough connection support, allowing different clients on LAN side to establish a secured IP Connection to the WAN server.



To enable IPSEC ALG, tick the checkbox and click the Save button.

5.5.6 SIP ALG

This page allows you to enable / disable SIP ALG.



5.6 Security

To display this function, you must enable the firewall feature in WAN Setup.
For detailed descriptions, with examples, please consult Appendix A - Firewall.

5.6.1 IP Filtering

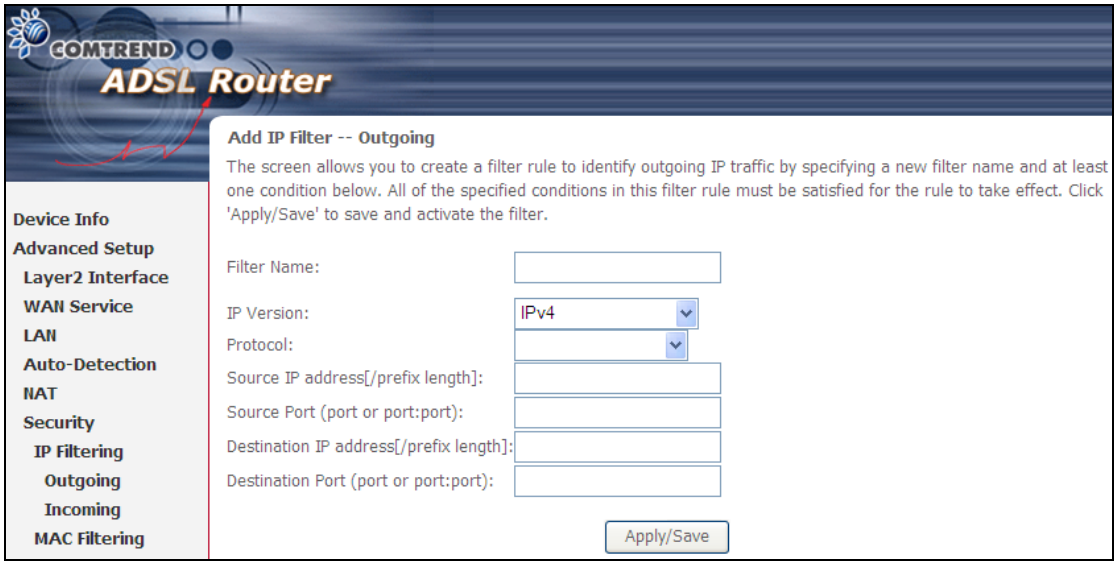
This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE:	This function is not available when in bridge mode. Instead, 5.6.2 MAC Filtering performs a similar function.

OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.

To add a filter (to block some outgoing IP traffic), click the **Add** button.
On the following screen, enter your filter criteria and then click **Apply/Save**.

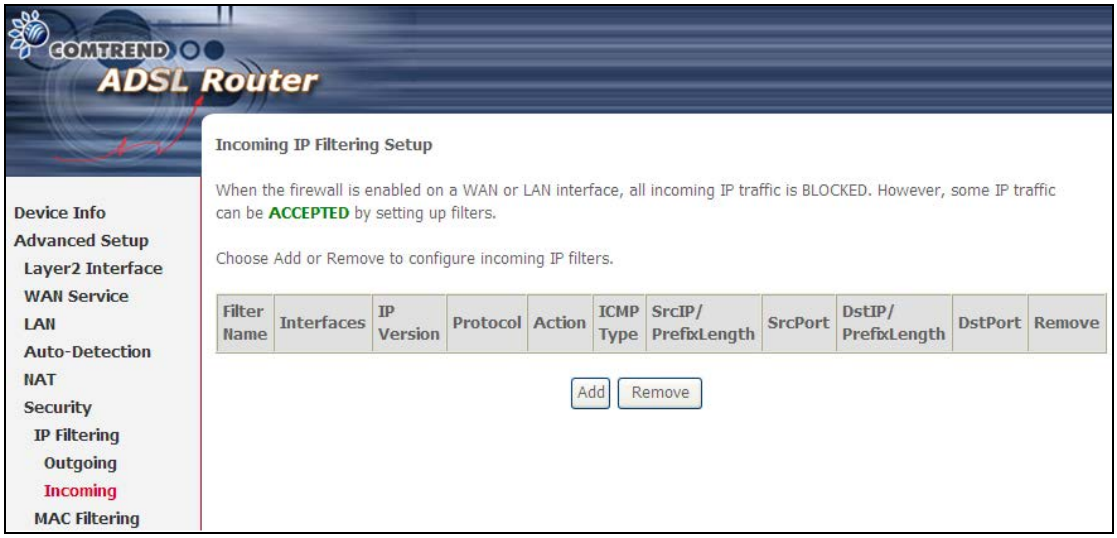

COMTREND
ADSL Router
Add IP Filter -- Outgoing
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Filter Name:
IP Version:
IPv4
Protocol:
Source IP address[/prefix length]:
Source Port (port or port:port):
Destination IP address[/prefix length]:
Destination Port (port or port:port):
Apply/Save
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
IP Filtering
Outgoing
Incoming
MAC Filtering

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

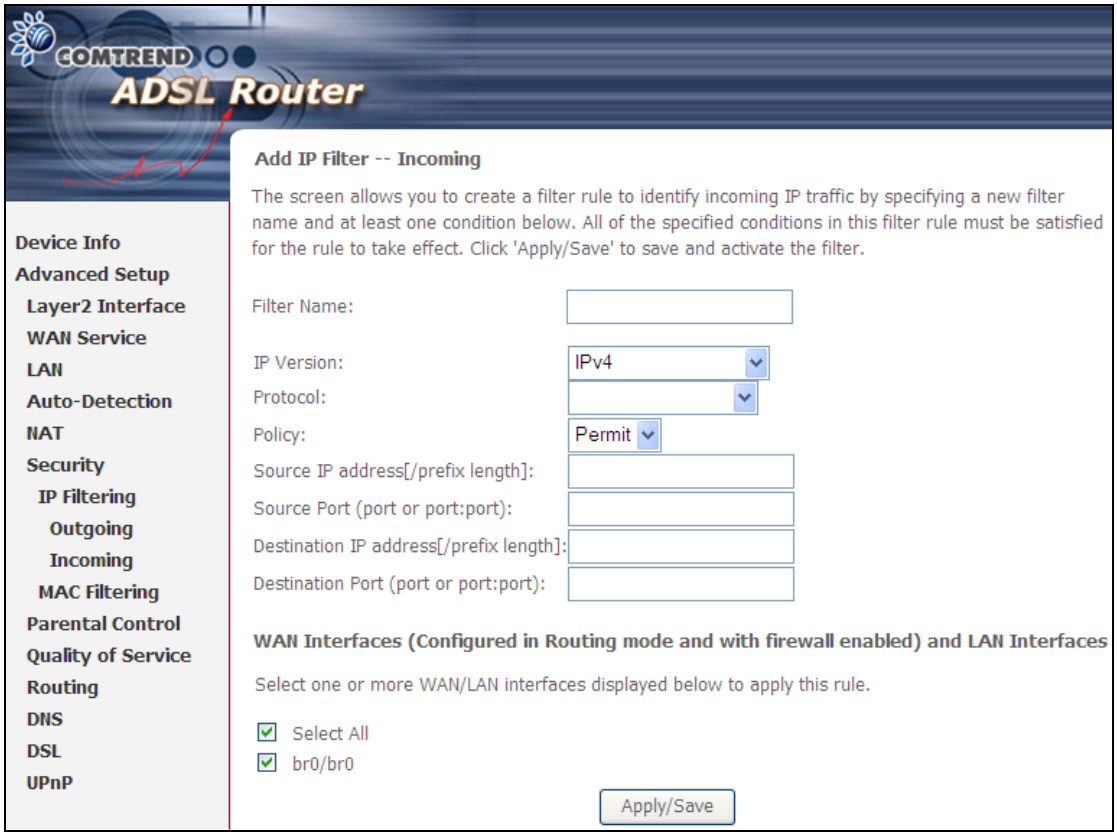
INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.



To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.



Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Policy	Permit/Drop packets specified by the firewall rule.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

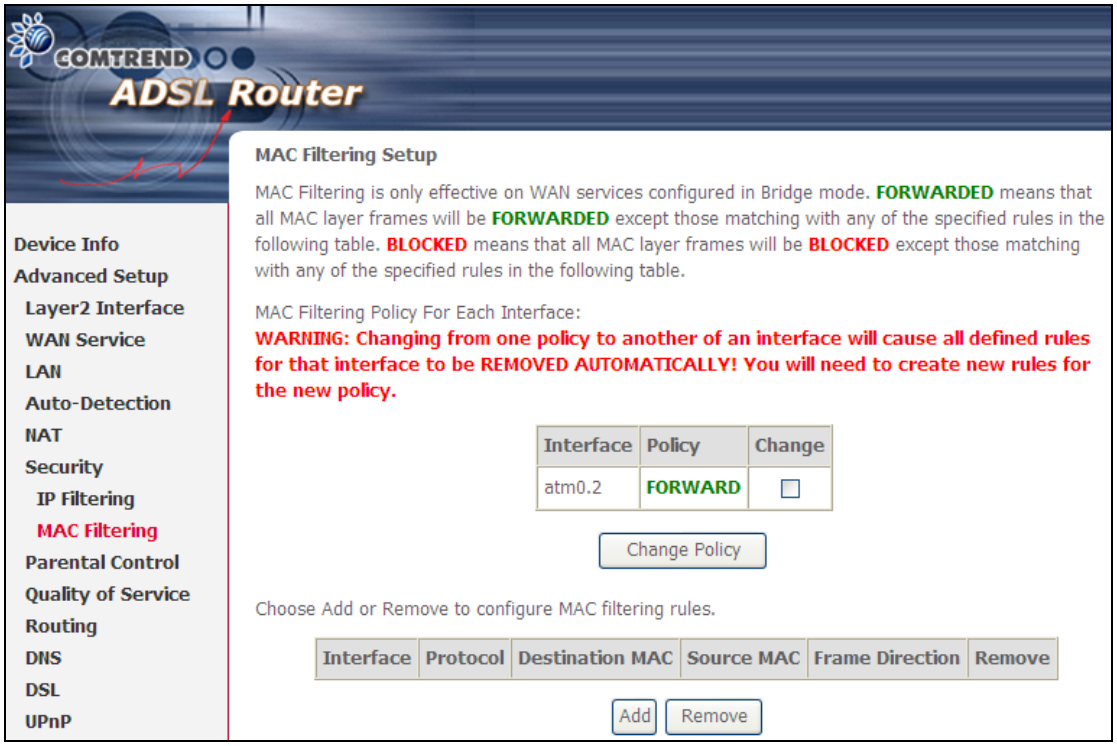
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

5.6.2 MAC Filtering

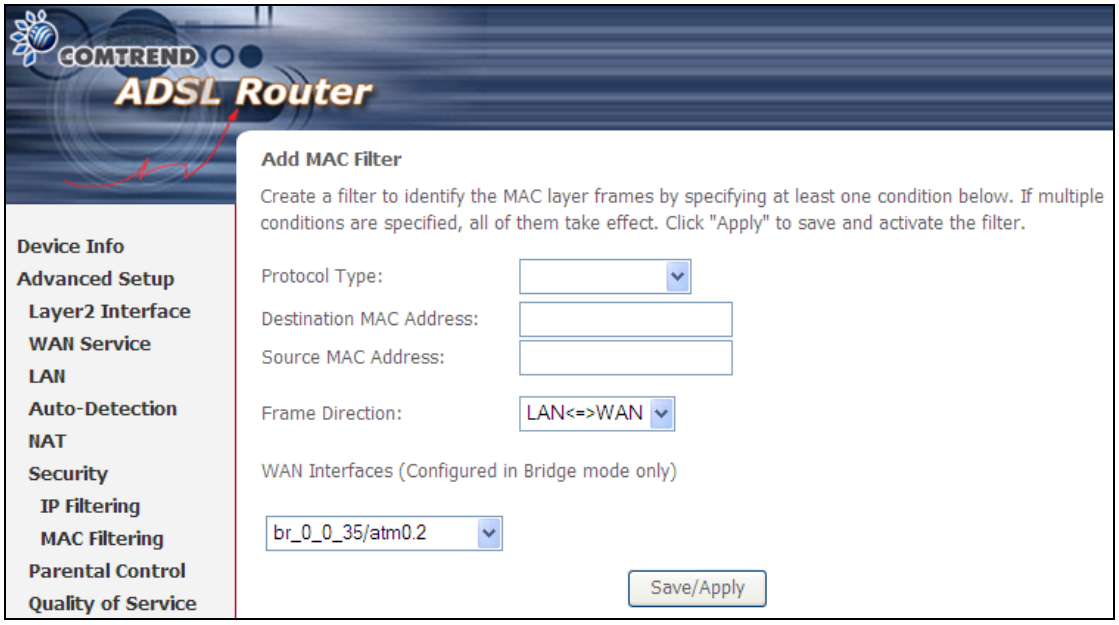
NOTE:	This option is only available in bridge mode. Other modes use 5.6.1 IP Filtering to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the AR-5389 can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
MAC Filtering Setup
MAC Filtering is only effective on WAN services configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
Interface
Policy
Change
atm0.2
FORWARD
Change Policy
Choose Add or Remove to configure MAC filtering rules.
Interface
Protocol
Destination MAC
Source MAC
Frame Direction
Remove
Add
Remove

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save / Apply** to save and activate the filter rule.



Consult the table below for detailed field descriptions.

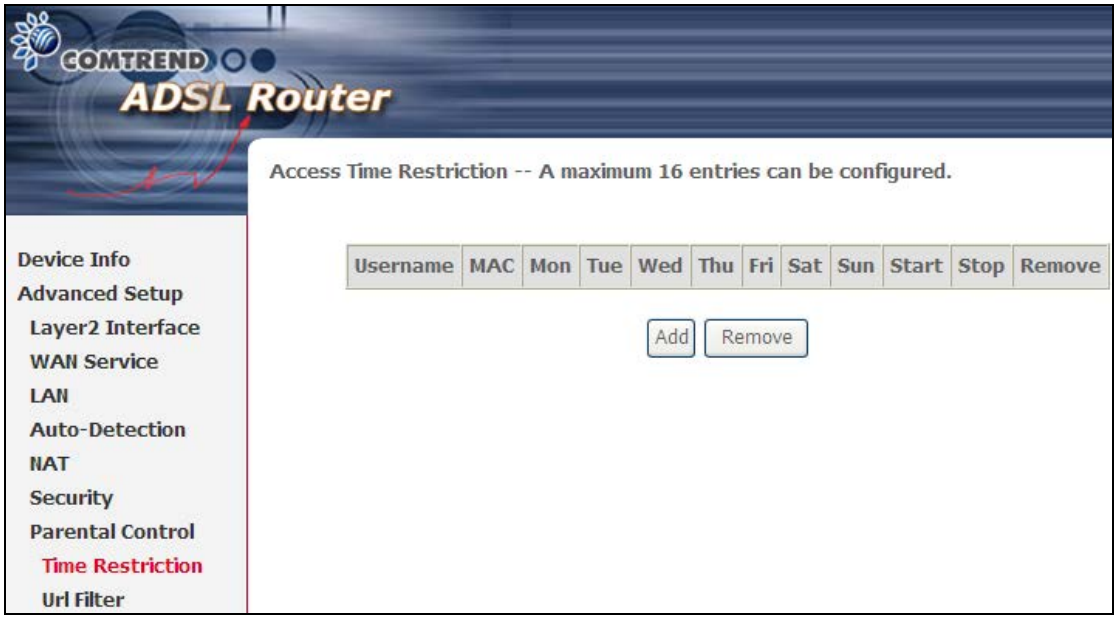
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface.

5.7 Parental Control

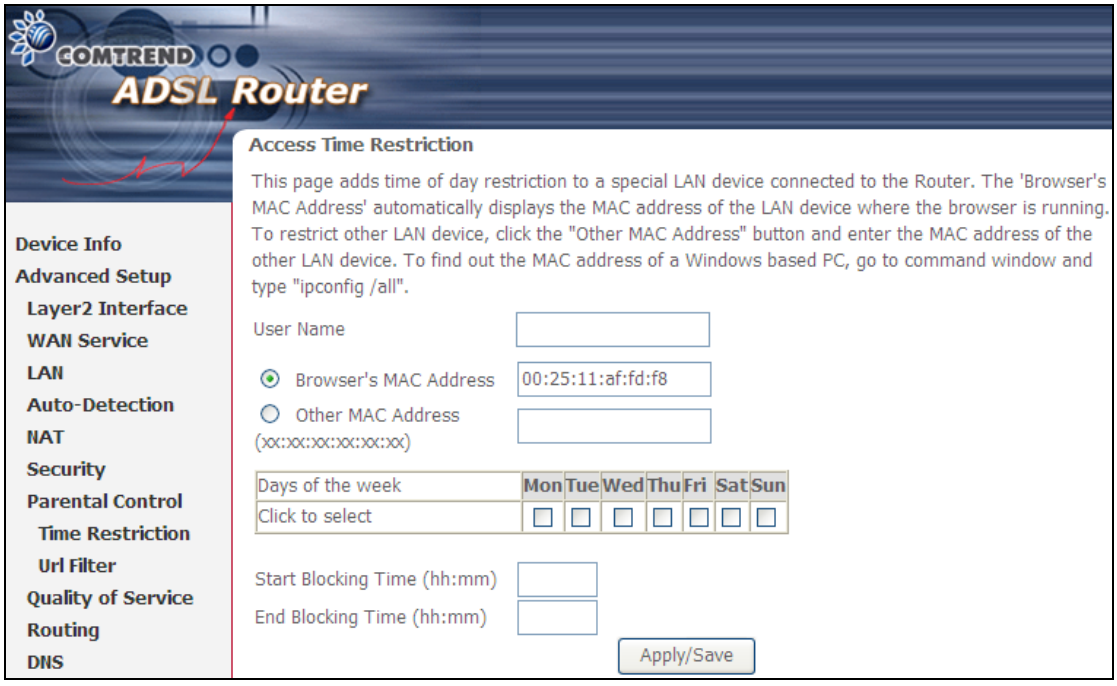
This selection provides WAN access control functionality.

5.7.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in 8.5 Internet Time, so that the scheduled times match your local time.



Click **Add** to display the following screen.


COMTREND
ADSL Router
Access Time Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Time Restriction
Url Filter
Quality of Service
Routing
DNS
User Name
Browser's MAC Address
00:25:11:af:fd:f8
Other MAC Address
(xx:xx:xx:xx:xx:xx)
Days of the week
Mon Tue Wed Thu Fri Sat Sun
Click to select
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Apply/Save

See below for field descriptions. Click **Apply / Save** to add a time restriction.

User Name: A user-defined label for this restriction.
Browser's MAC Address: MAC address of the PC running the browser.
Other MAC Address: MAC address of another LAN device.
Days of the Week: The days the restrictions apply.
Start Blocking Time: The time the restrictions start.
End Blocking Time: The time the restrictions end.

5.7.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.

Select URL List Type: Exclude or Include. Then click **Add** to display the following screen.

Parental Control -- URL Filter Add
Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.
URL Address: www.yahoo.com
Port Number: 80
(Default 80 will be applied if leave blank.)
Save/Apply

Enter the URL address and port number then click **Save / Apply** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.

A maximum of 100 entries can be added to the URL Filter list.
Tick the **Exclude** radio button to deny access to the websites listed.
Tick the **Include** radio button to restrict access to only those listed websites.

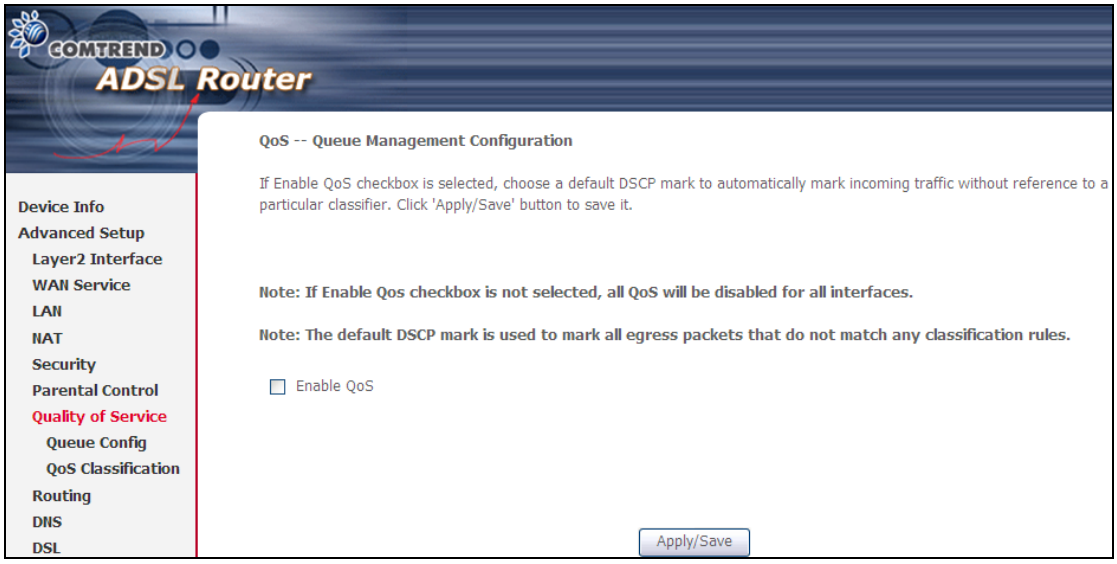
5.8 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.
(See Appendix E - Connection Setup for detailed PVC setup instructions).

5.8.1 Queue Management Configuration

To Enable QoS tick the checkbox ☑ and select a Default DSCP Mark.

Click **Apply / Save** to activate QoS.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
Parental Control
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Apply/Save

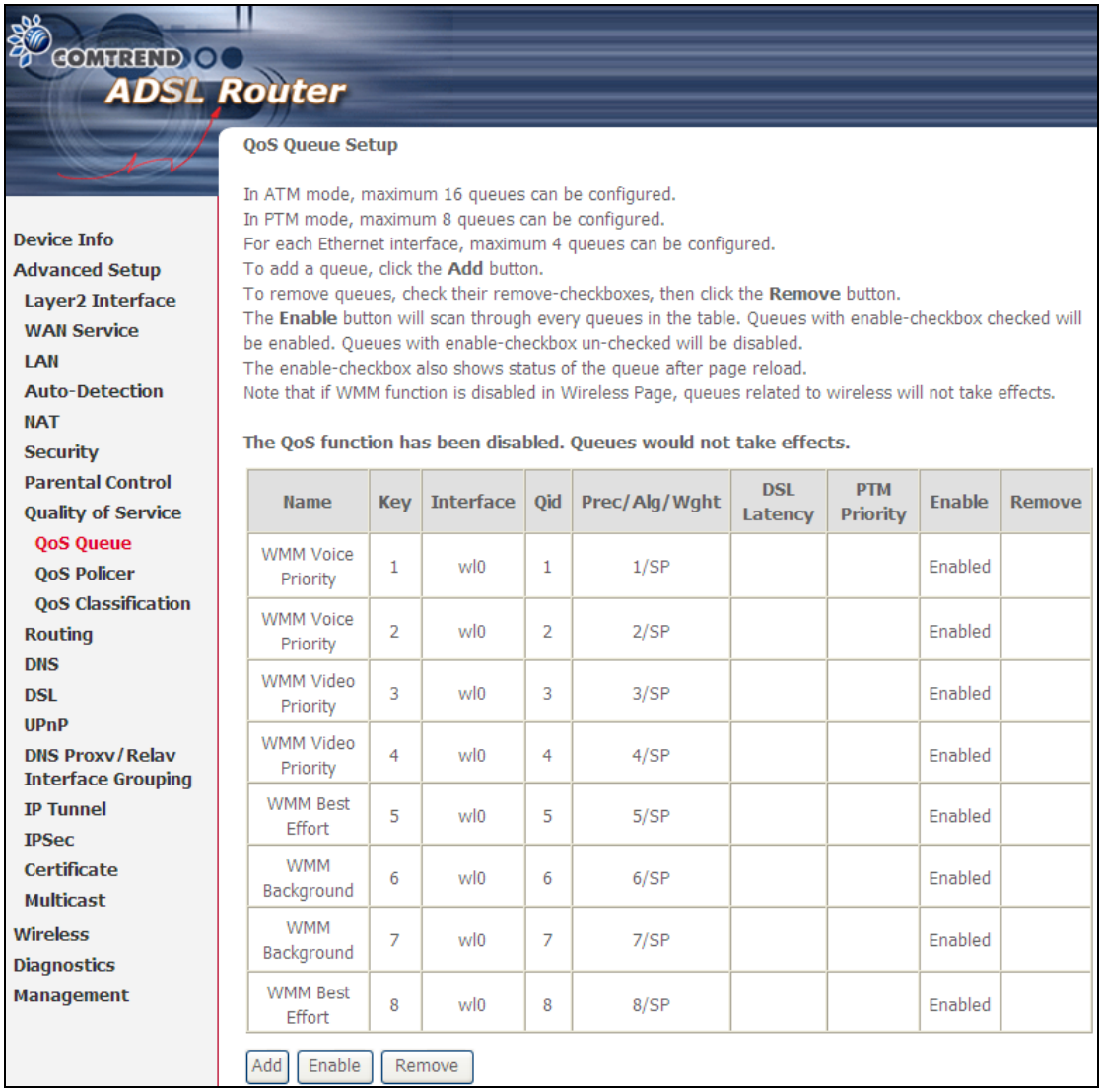
QoS and **DSCP Mark** are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

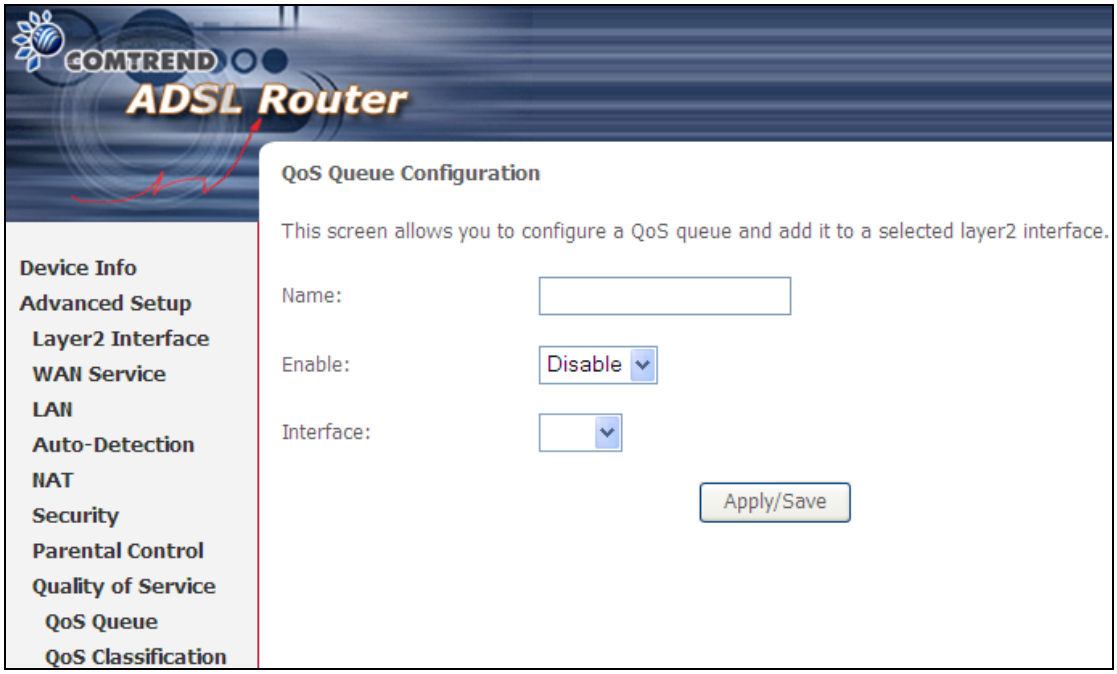
Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

5.8.2 Queue Configuration

This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
UPnP
DNS Proxy/Relay
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
QoS Queue Setup
In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
To add a queue, click the Add button.
To remove queues, check their remove-checkboxes, then click the Remove button.
The Enable button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.
The QoS function has been disabled. Queues would not take effects.
Name
Key
Interface
Qid
Prec/Alg/Wght
DSL Latency
PTM Priority
Enable
Remove
WMM Voice Priority 1 wl0 1 1/SP Enabled
WMM Voice Priority 2 wl0 2 2/SP Enabled
WMM Video Priority 3 wl0 3 3/SP Enabled
WMM Video Priority 4 wl0 4 4/SP Enabled
WMM Best Effort 5 wl0 5 5/SP Enabled
WMM Background 6 wl0 6 6/SP Enabled
WMM Background 7 wl0 7 7/SP Enabled
WMM Best Effort 8 wl0 8 8/SP Enabled
Add
Enable
Remove

Click **Enable** to activate the QoS Queue. Click **Add** to display the following screen.



Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

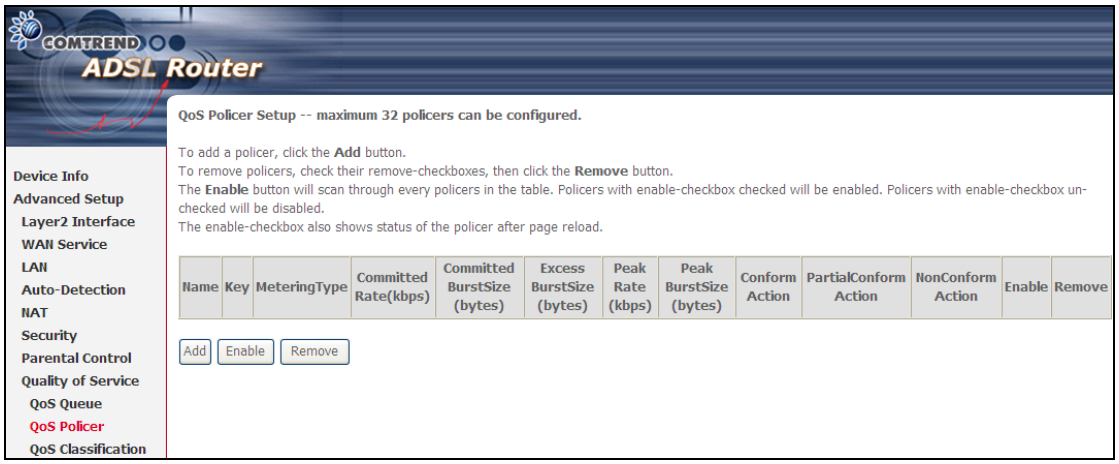
Interface: Assign the entry to a specific network interface (QoS enabled).

5.8.3 QoS Policer

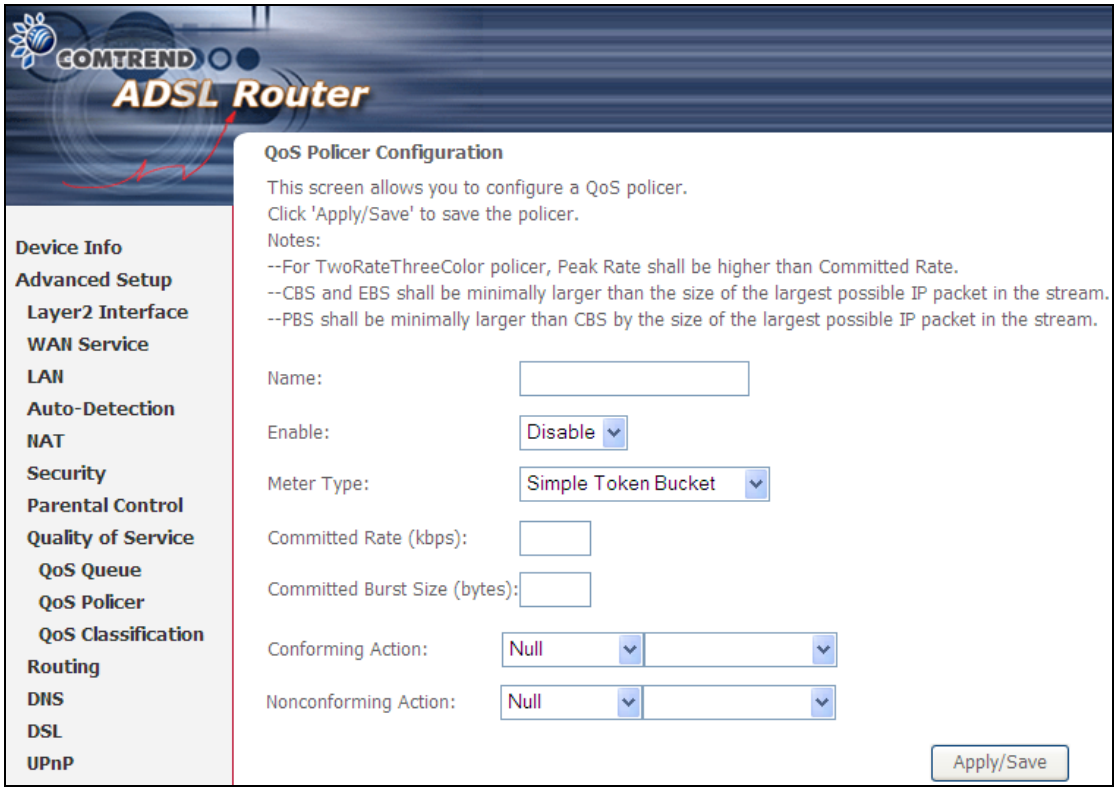
To remove policers, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the policer after page reload.



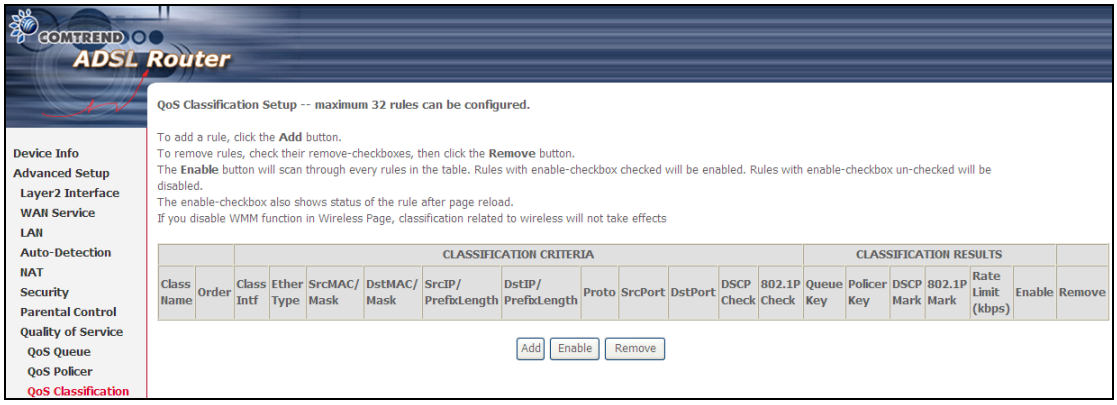
To add a policer, click the **Add** button.



Field	Description
Name	Name of this policer rule
Enable	Enable/Disable this policer rule
Meter Type	Meter type used for this policer rule
Committed Rate (kbps)	Defines the rate allowed for committed packets
Committed Burst Size (bytes)	Maximum amount of packets that can be processed by this policer
Conforming Action	Defines action to be taken if packets match this policer
Nonconforming Action	Defines actions to be taken if packets do not match this policer

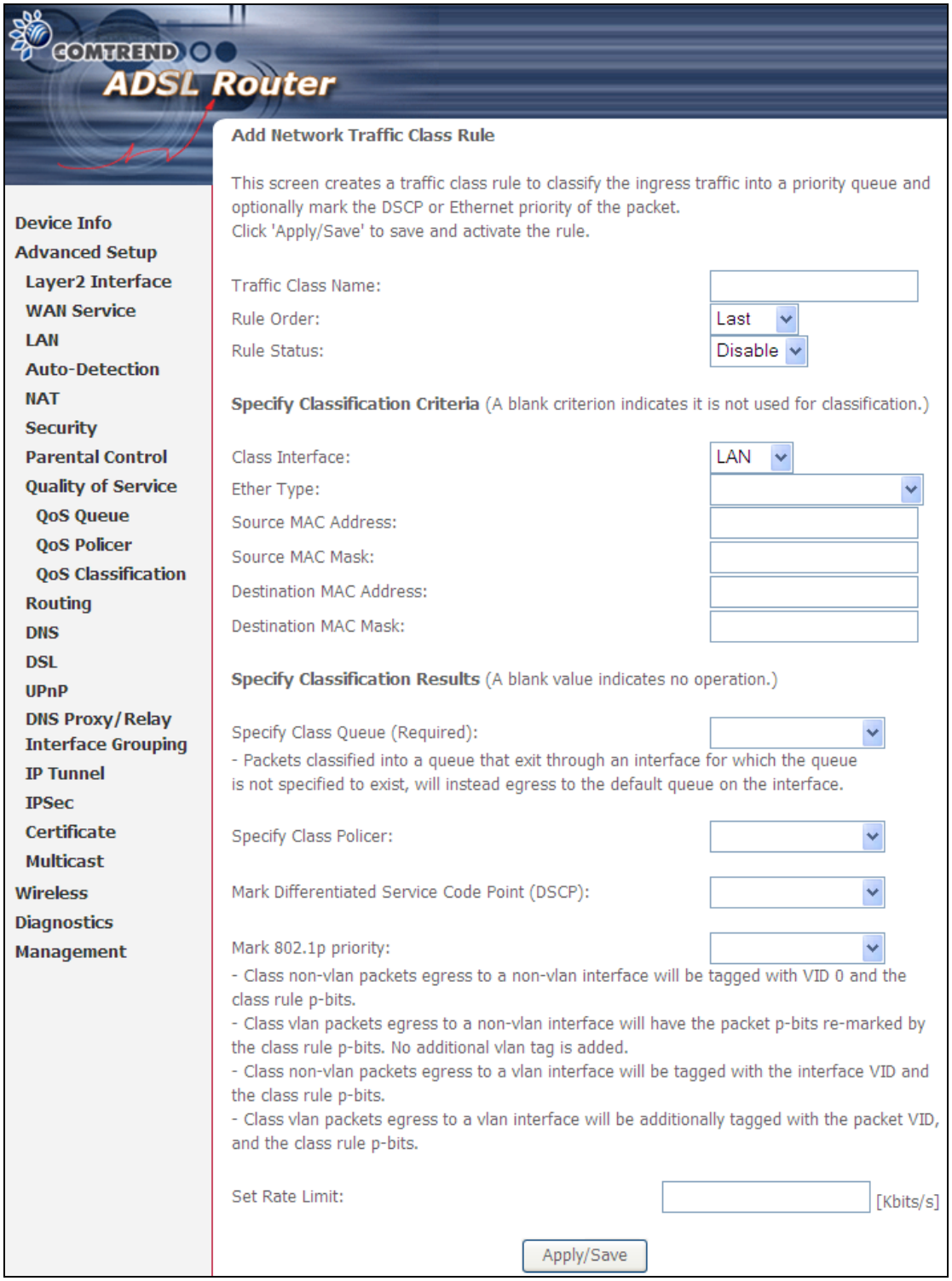
5.8.4 QoS Classification

The network traffic classes are listed in the following table.



Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one logical condition. All the conditions specified in the rule must be satisfied for it to take effect.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
UPnP
DNS Proxy/Relay
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Add Network Traffic Class Rule
This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
Click 'Apply/Save' to save and activate the rule.
Traffic Class Name:
Rule Order:
Last
Rule Status:
Disable
Specify Classification Criteria (A blank criterion indicates it is not used for classification.)
Class Interface:
LAN
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
Specify Classification Results (A blank value indicates no operation.)
Specify Class Queue (Required):
- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.
Specify Class Policer:
Mark Differentiated Service Code Point (DSCP):
Mark 802.1p priority:
- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.
Set Rate Limit:
[Kbits/s]
Apply/Save

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).

Field	Description
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Specify Class Queue	Select corresponding queue to deliver outgoing traffic.
Specify Class Policer	Packets classified into a policer will be marked based on the conforming action of the policer.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. Lower values have higher priority.

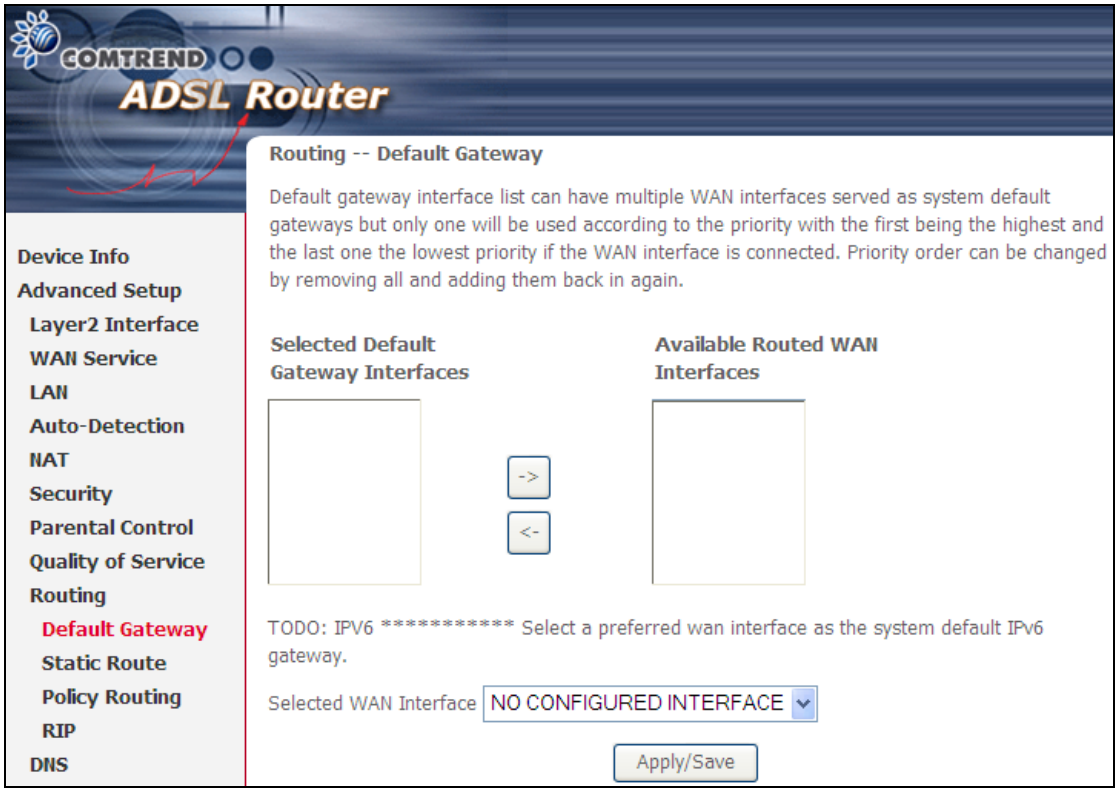
5.9 Routing

These following routing functions are accessed from this menu:
Default Gateway, Static Route, Policy Routing and **RIP**.

NOTE:	In bridge mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.

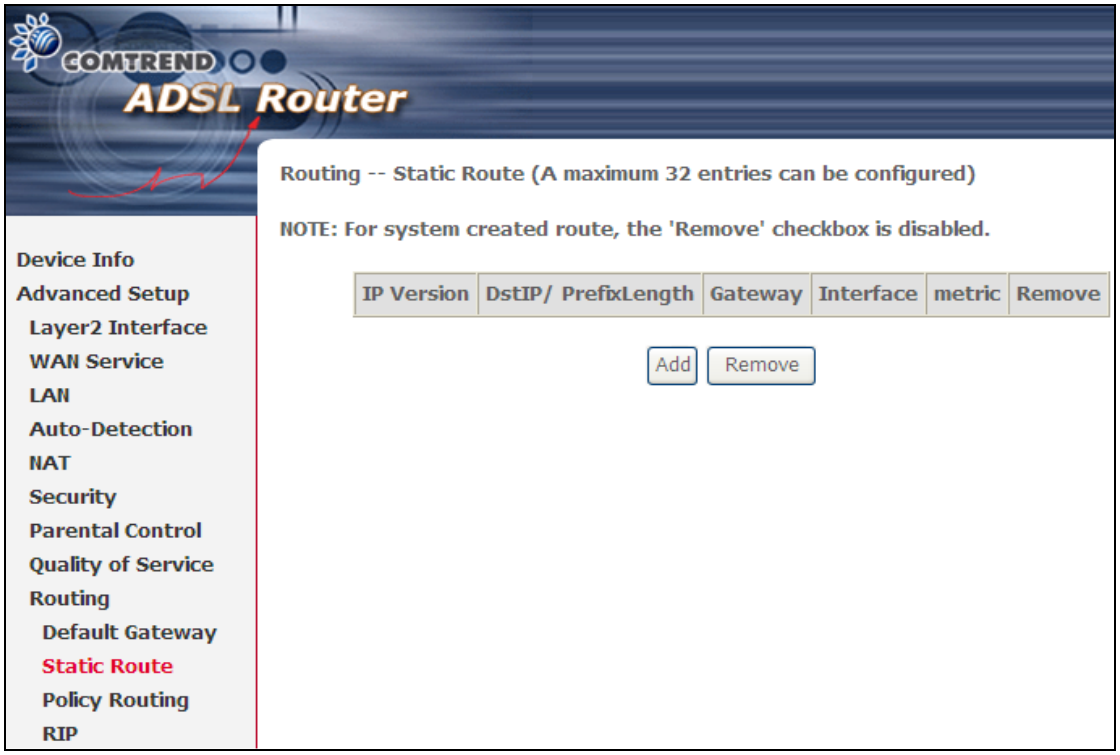
5.9.1 Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

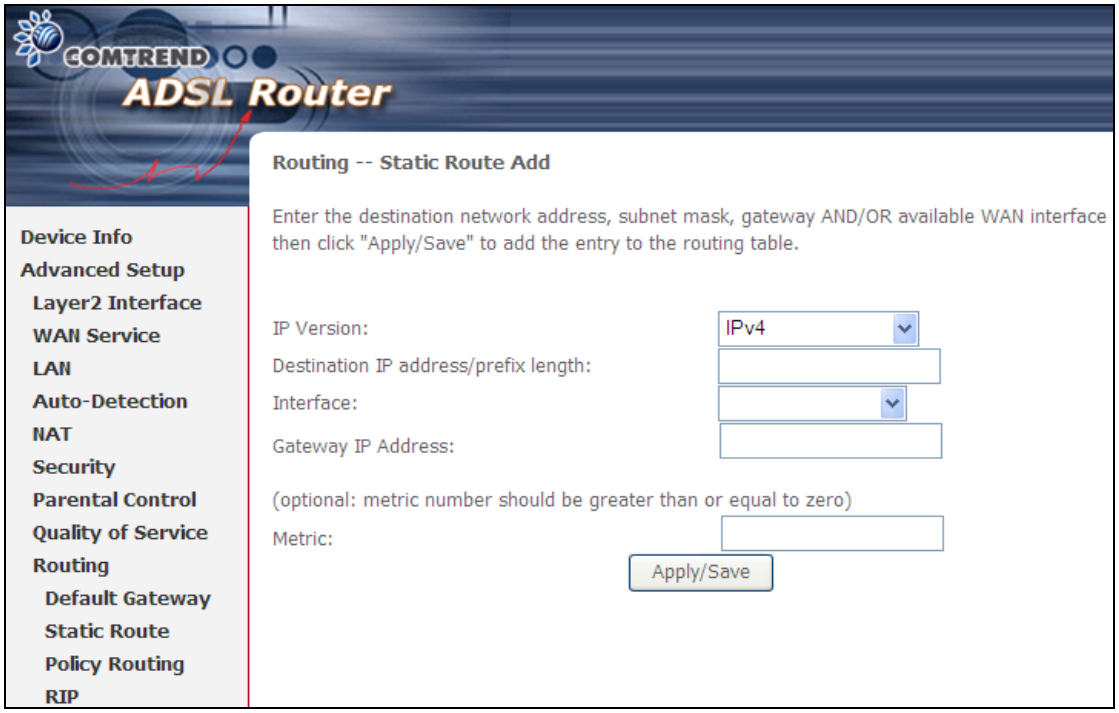

COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
DNS
Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
->
<-
TODO: IPV6 ********** Select a preferred wan interface as the system default IPv6 gateway.
Selected WAN Interface
NO CONFIGURED INTERFACE
Apply/Save

5.9.2 Static Route

This option allows for the configuration of static routes by destination IP.
Click **Add** to create a static route or click **Remove** to delete a static route.



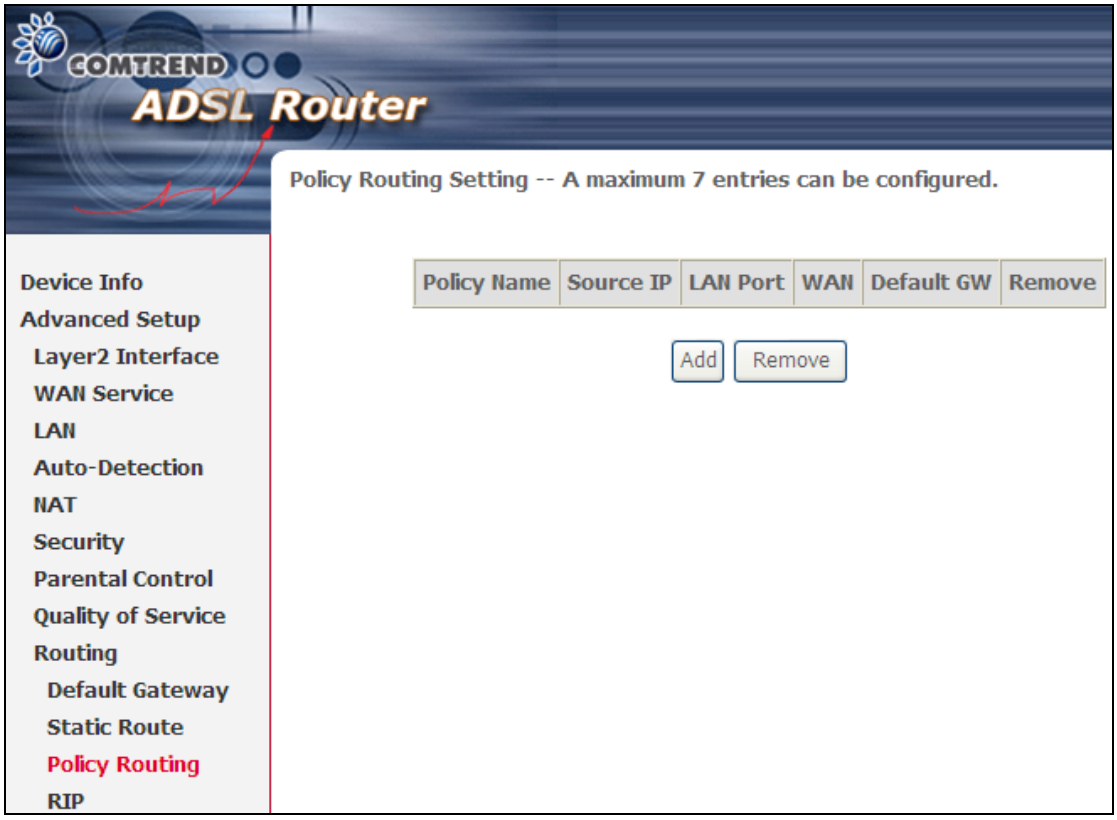
After clicking **Add** the following screen will display.



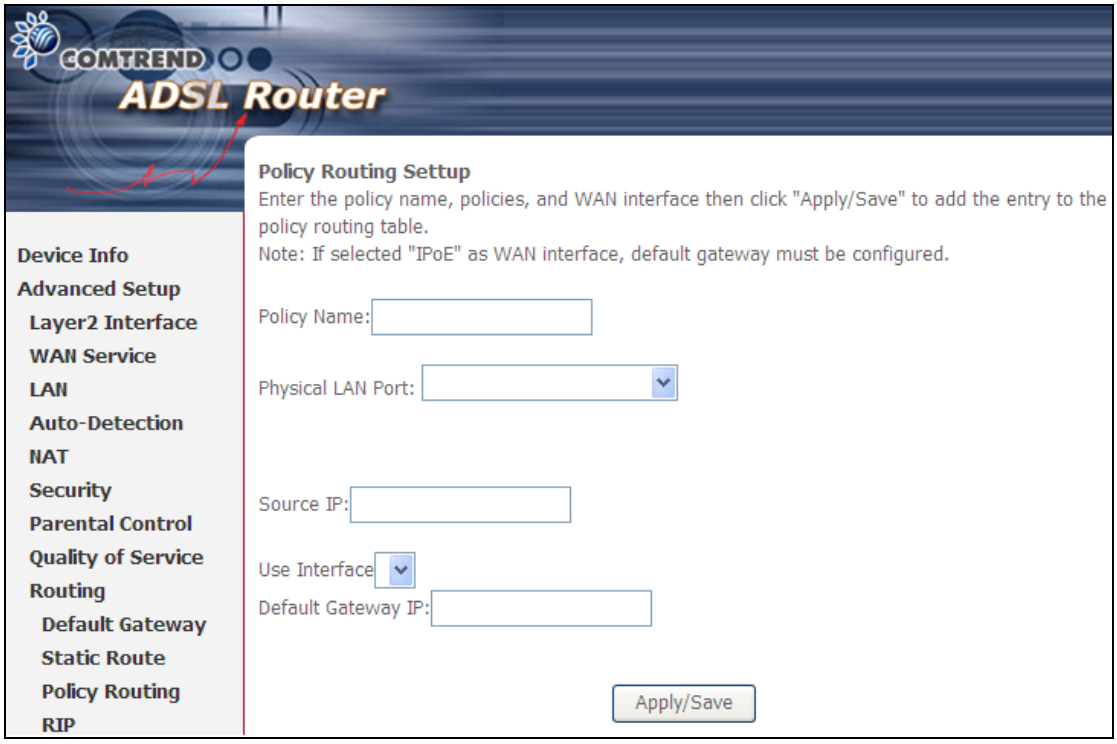
Input the Destination IP Address, select the interface type, Input the Gateway IP, (and the Metric number if required). Then, click **Apply / Save** to add an entry to the routing table.

5.9.3 Policy Routing

This option allows for the configuration of static routes by policy.
Click **Add** to create a routing policy or **Remove** to delete one.



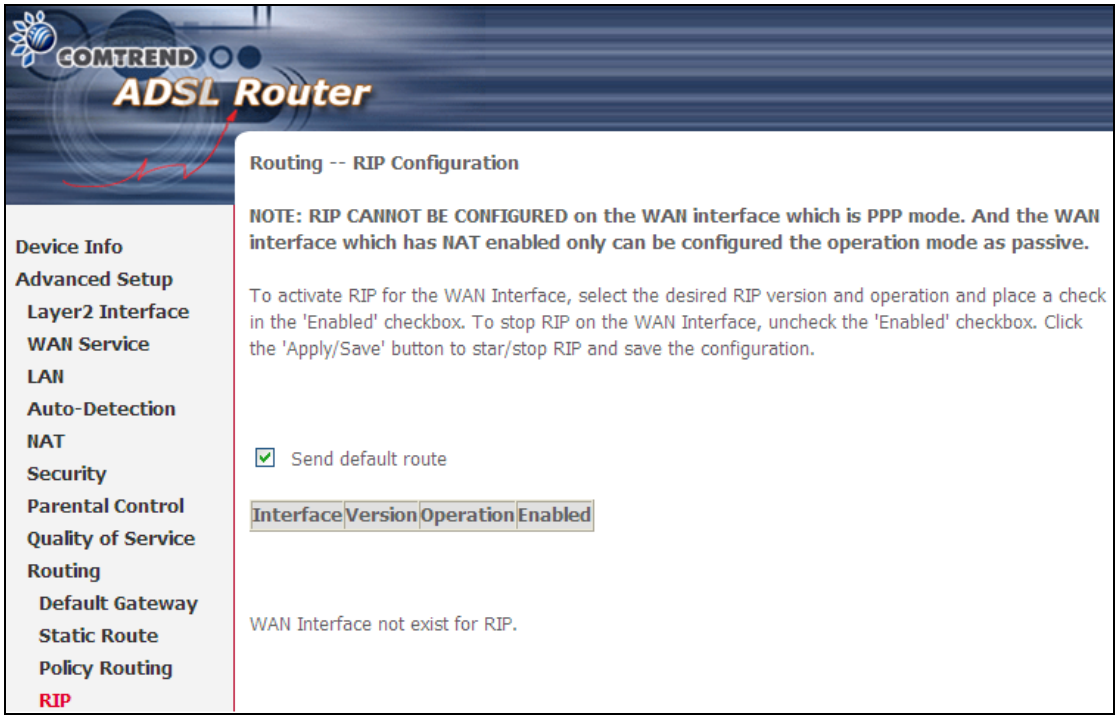
On the following screen, complete the form and click **Apply / Save** to create a policy.



Field	Description
Policy Name	Name of the route policy
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Interface that traffic will be directed to
Default Gateway IP	IP Address of the default gateway

5.9.4 RIP

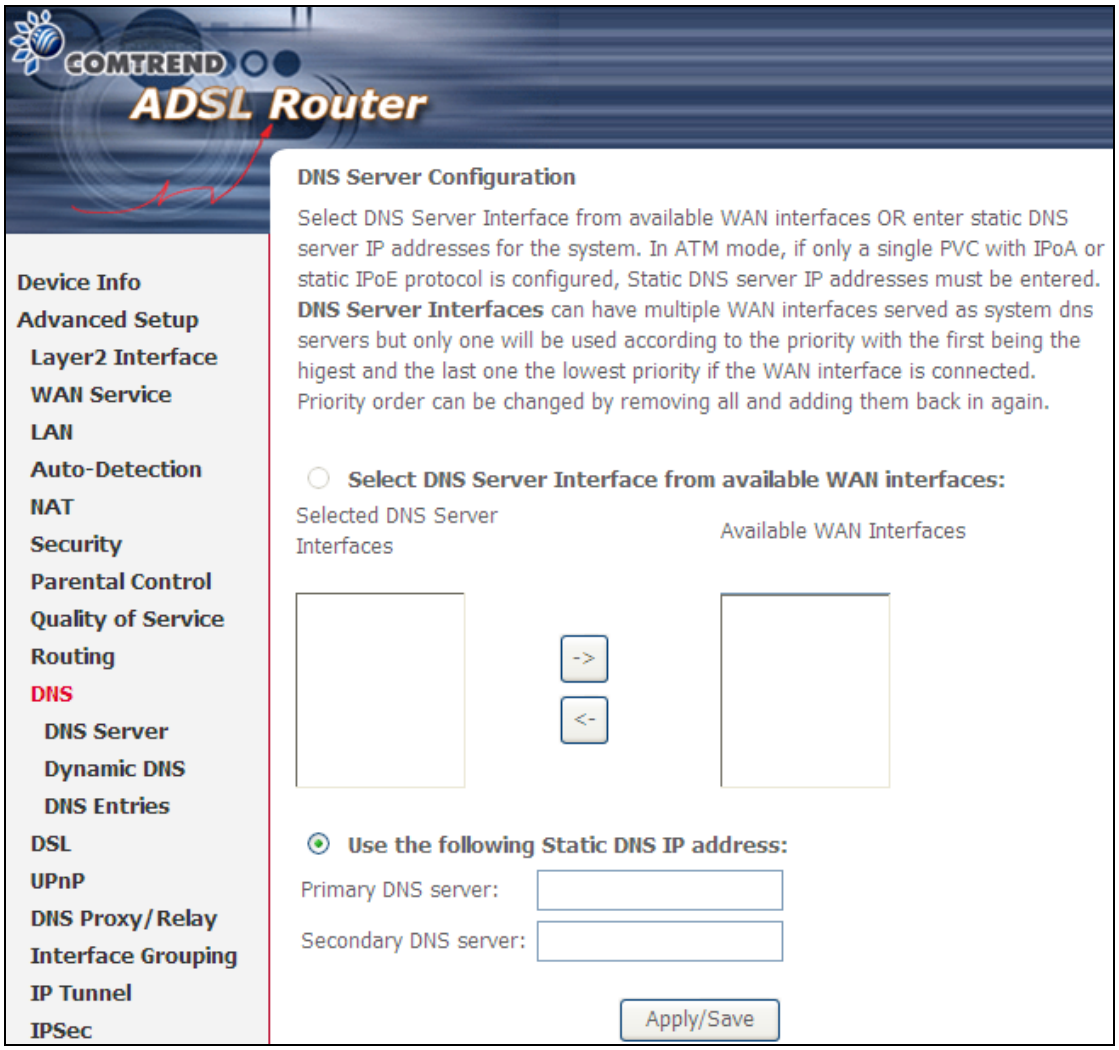
To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox ☑ for at least one WAN interface before clicking **Save / Apply**.

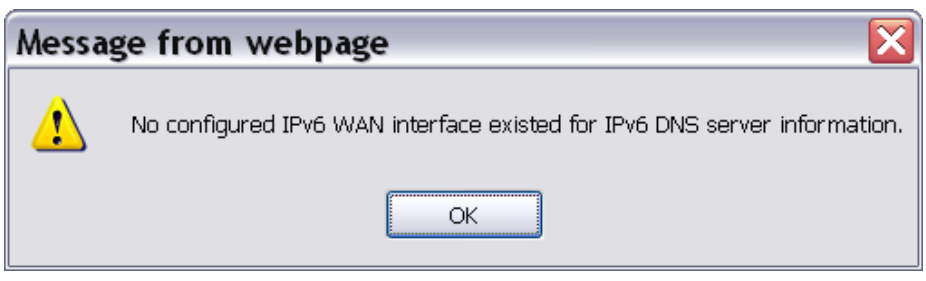

COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
Routing -- RIP Configuration
NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.
Send default route
Interface Version Operation Enabled
WAN Interface not exist for RIP.

5.10 DNS

5.10.1 DNS Server

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. **DNS Server Interfaces** can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

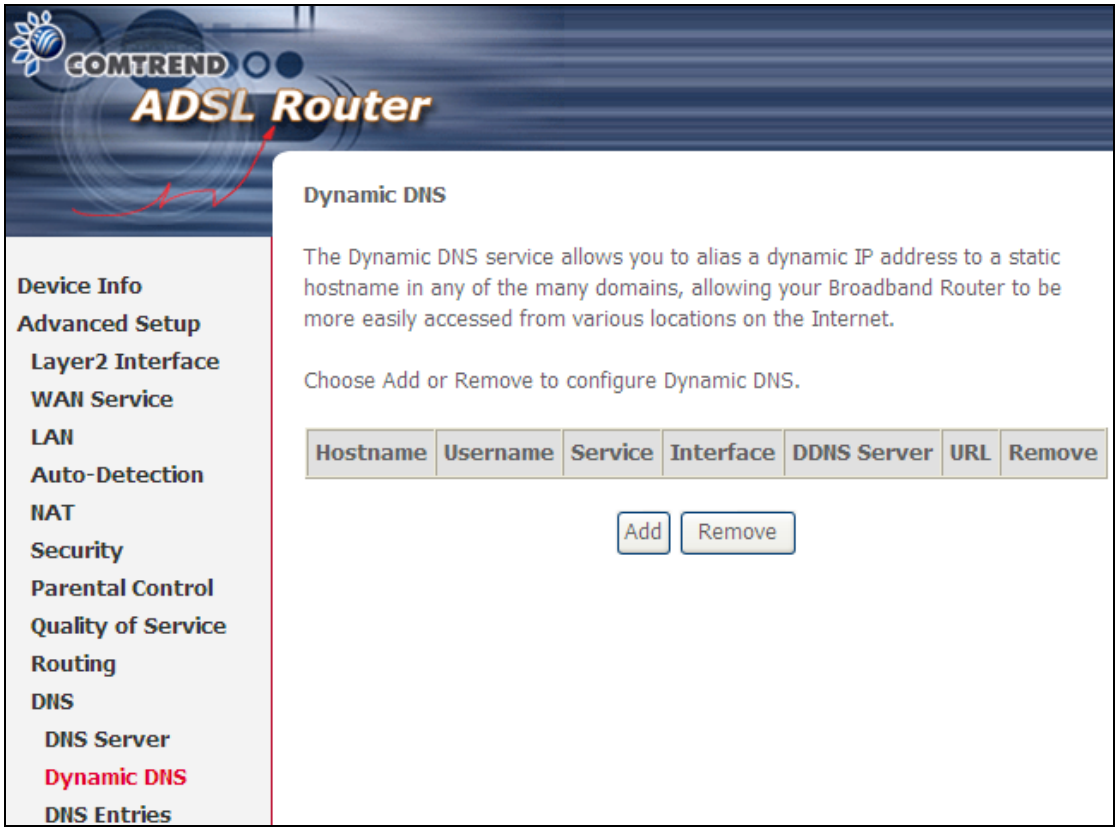

COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DSL
UPnP
DNS Proxy/Relay
Interface Grouping
IP Tunnel
IPSec
DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Apply/Save



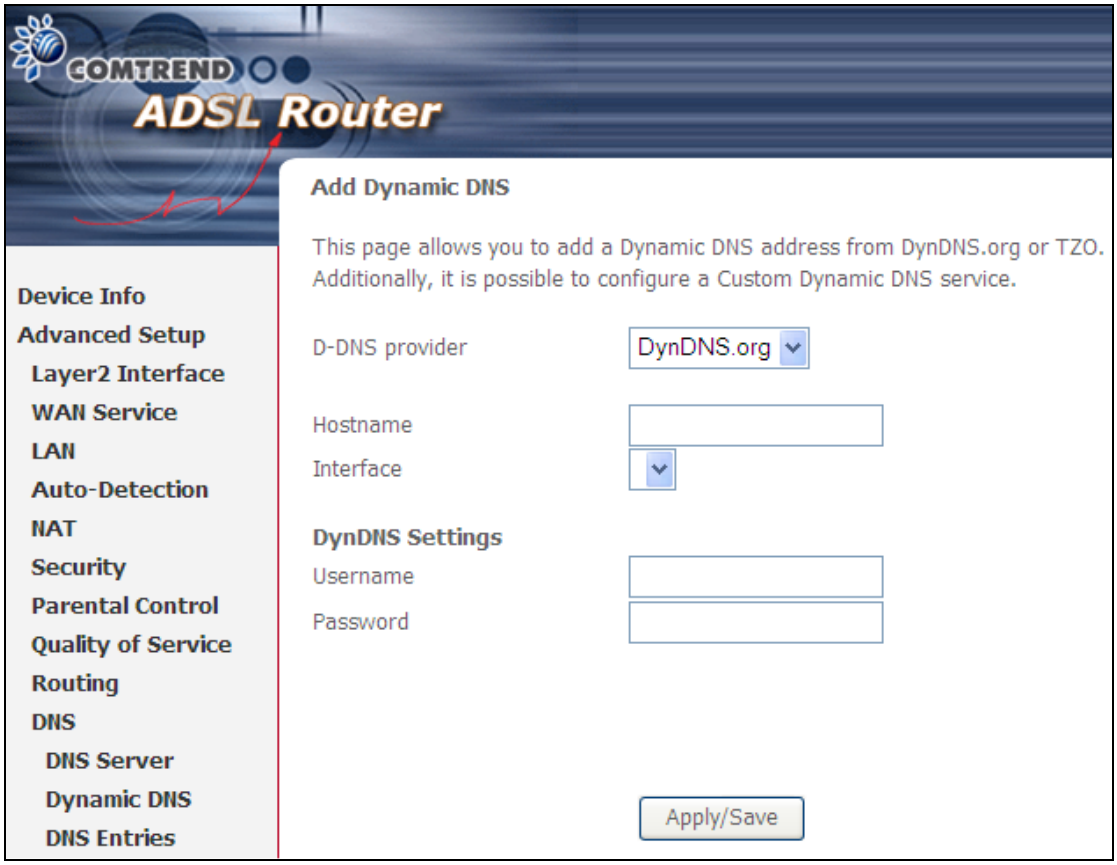
If is no IPv6 WAN interface is configured, a warning message system will pop up when accessing DNS Server.

5.10.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the AR-5389 to be more easily accessed from various locations on the Internet.



To add a dynamic DNS service, click **Add**. The following screen will display.



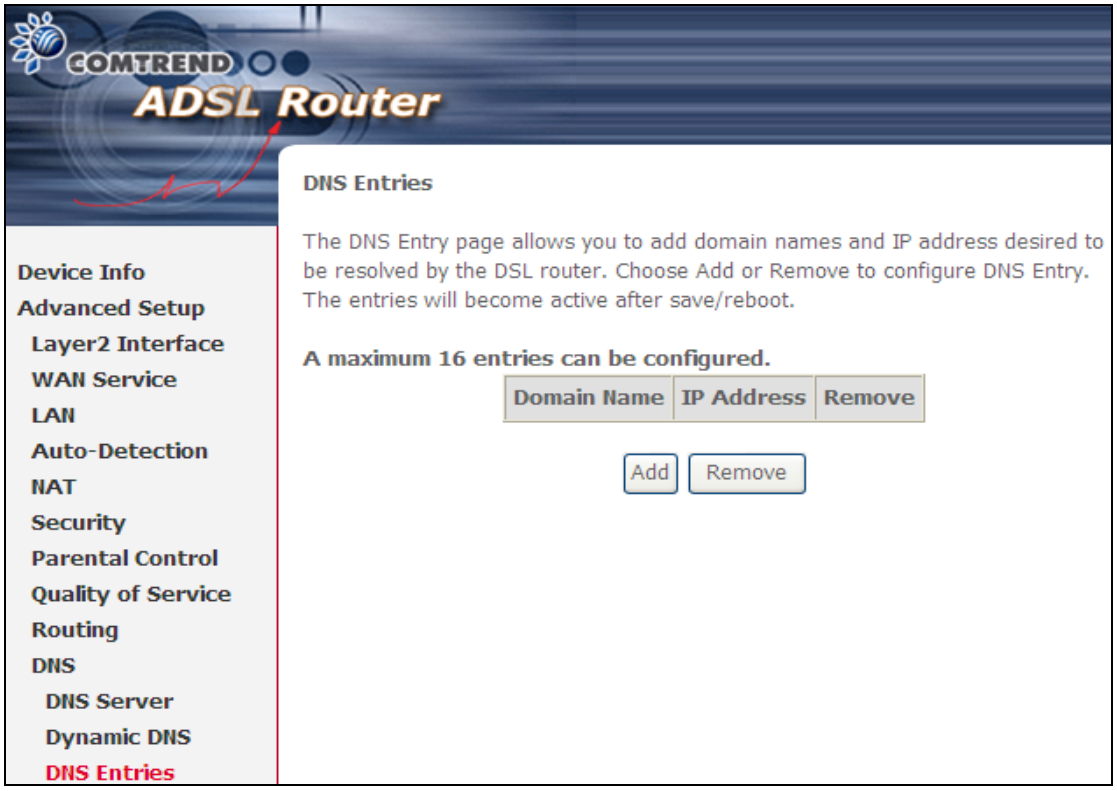
Make your settings and click the **Apply / Save** button.

Consult the table below for field descriptions.

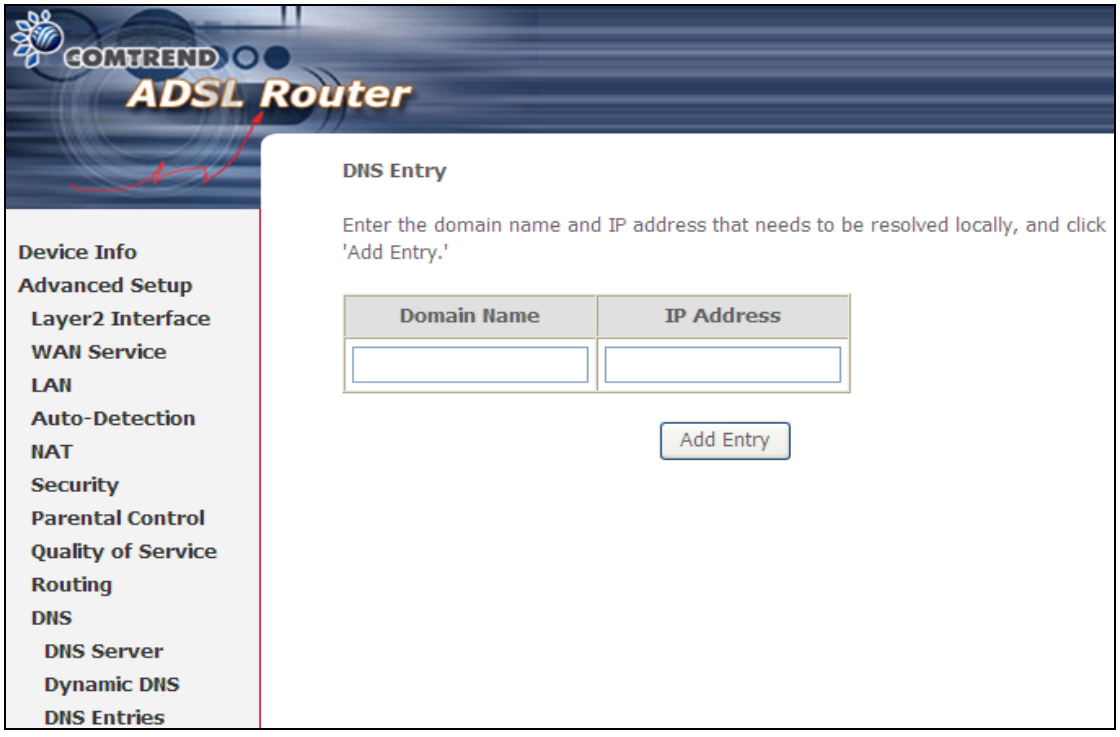
Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

5.10.3 DNS Entries

The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router.



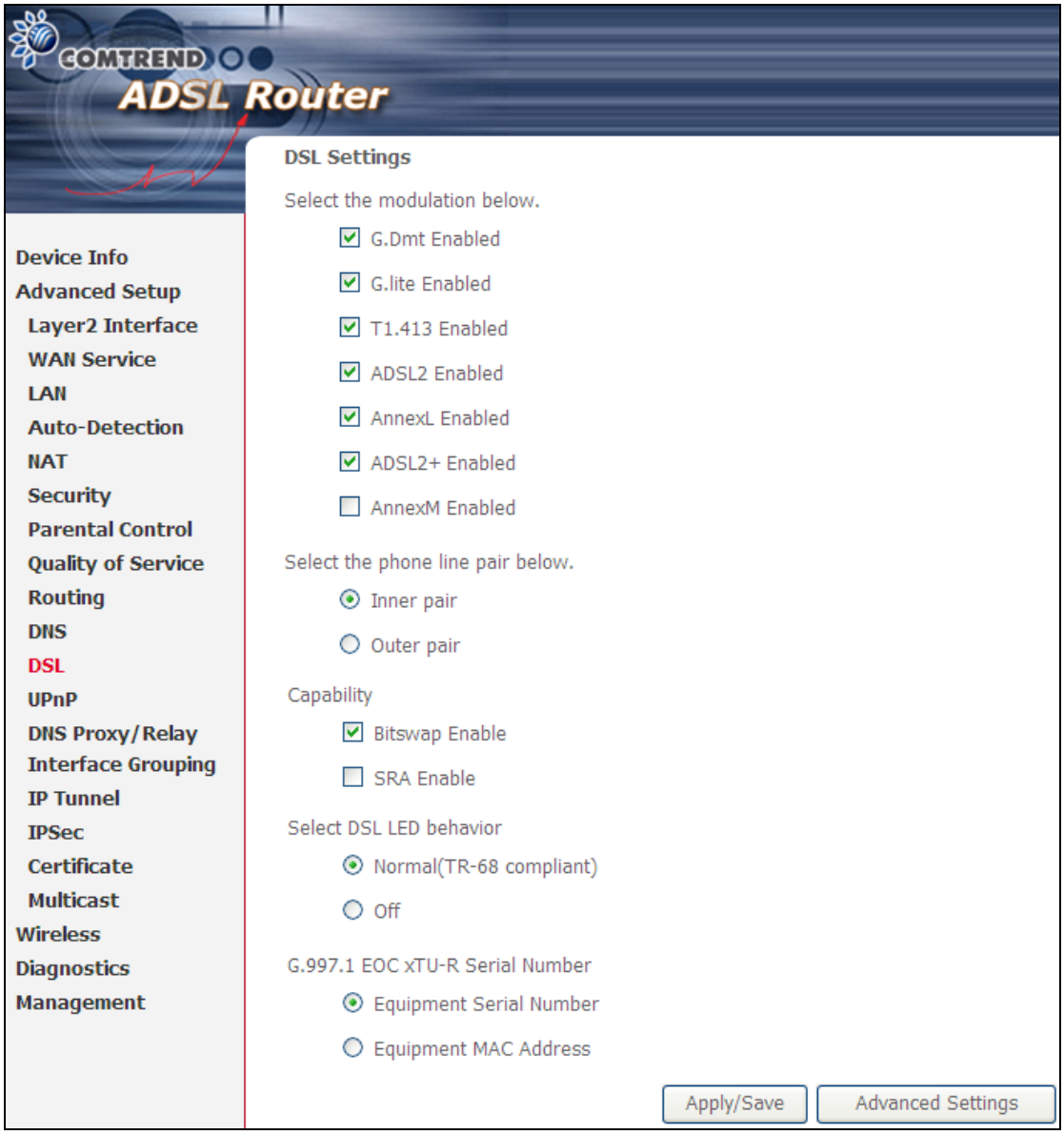
Choose Add or Remove to configure DNS Entry. The entries will become active after save/reboot.



Enter the domain name and IP address that needs to be resolved locally, and click the **Add Entry** button.

5.11 DSL

The DSL Settings screen allows for the selection of DSL modulation modes.
For optimum performance, the modes selected should match those of your ISP.

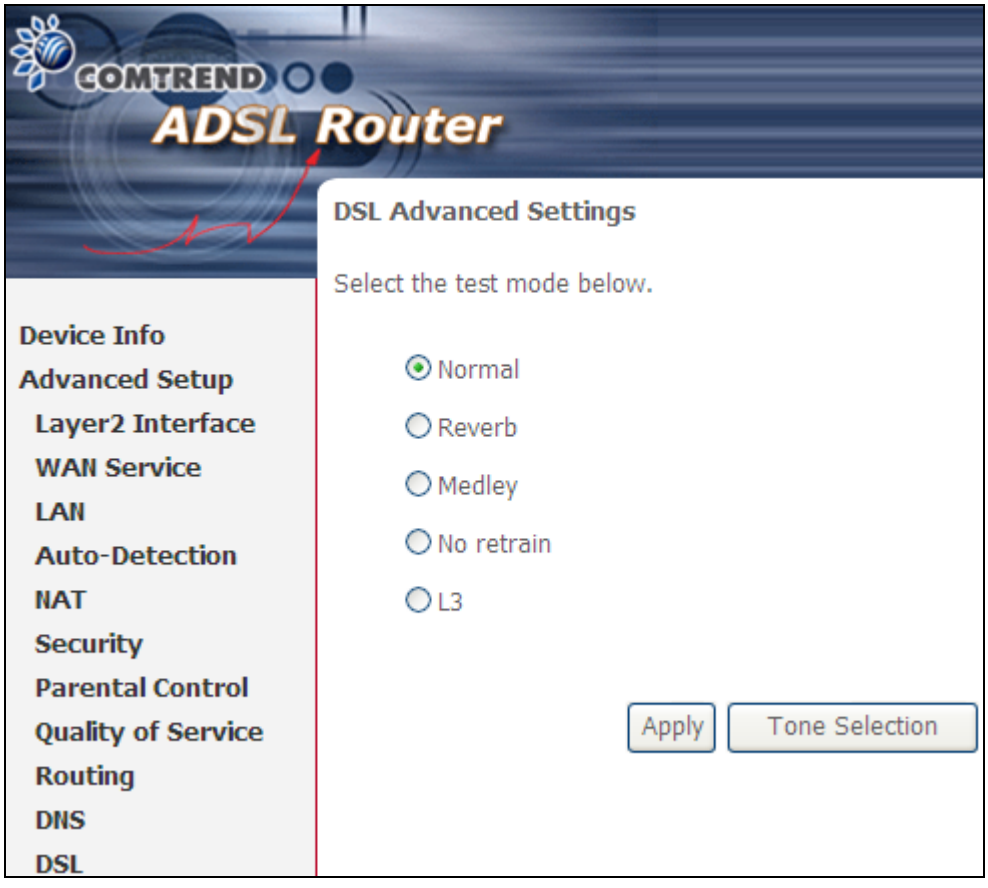


DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
G.Dmt	Downstream: 12 Mbps Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates
ADSL2+	Downstream: 24 Mbps Upstream: 1.0 Mbps

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
AnnexM	Downstream: 24 Mbps Upstream: 3.5 Mbps
Options	**Description**
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
DSL LED behavior	Normal (TR-68 compliant) – DSL LED blink/on/off following TR-68 standard Off – always turn off DSL LED
G997.1 EOC xTU-R Serial Number	Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options. On the following screen you can select a test mode or modify tones by clicking **Tone Selection**. Click **Apply** to implement these settings and return to the previous screen.



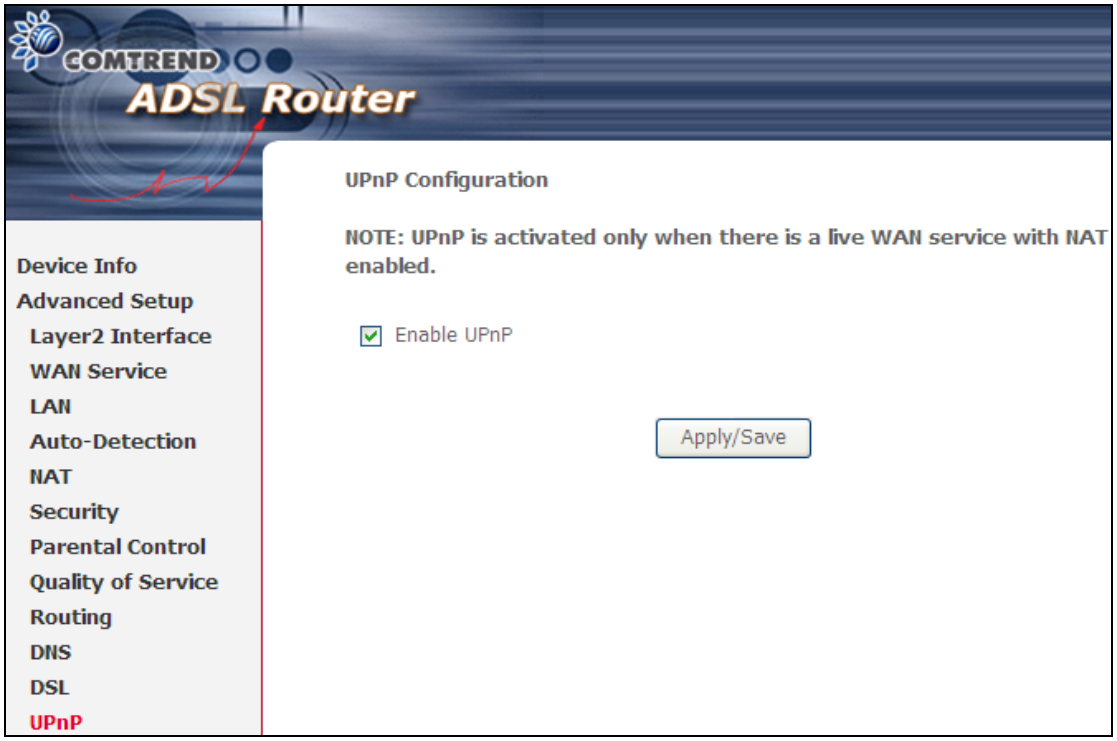
On this screen you select the tones you want activated, then click **Apply**.

Field	Description
Normal	DSL line signal is detected and sent normally

Field	Description
Reverb	DSL line signal is sent continuously in reverb mode
Medley	DSL line signal is sent continuously in medley mode
No Retrain	DSL line signal will always be on even when DSL line is unplugged
L3	DSL line is set in L3 power mode

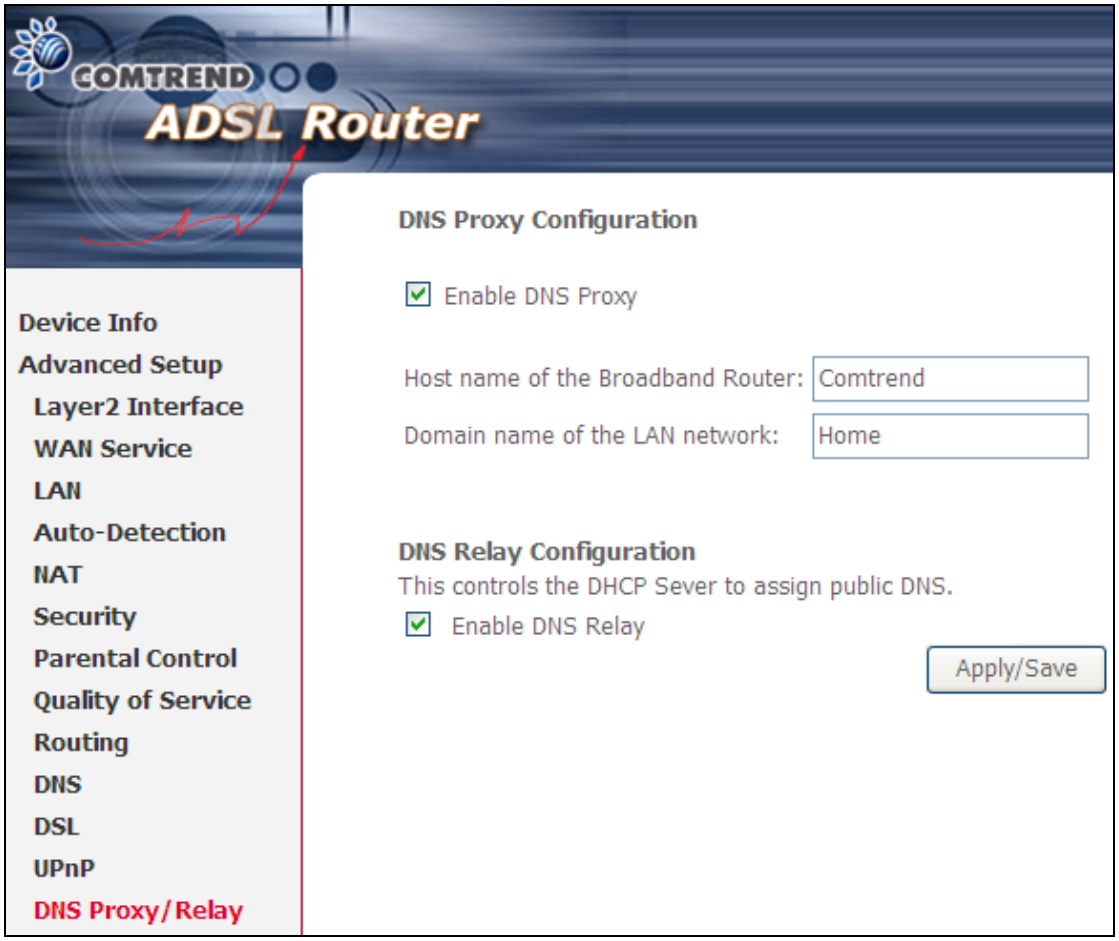
5.12 UPnP

Select the checkbox ☑ provided and click **Apply / Save** to enable UPnP protocol.



5.13 DNS Proxy/Relay

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "Comtrend.Home".

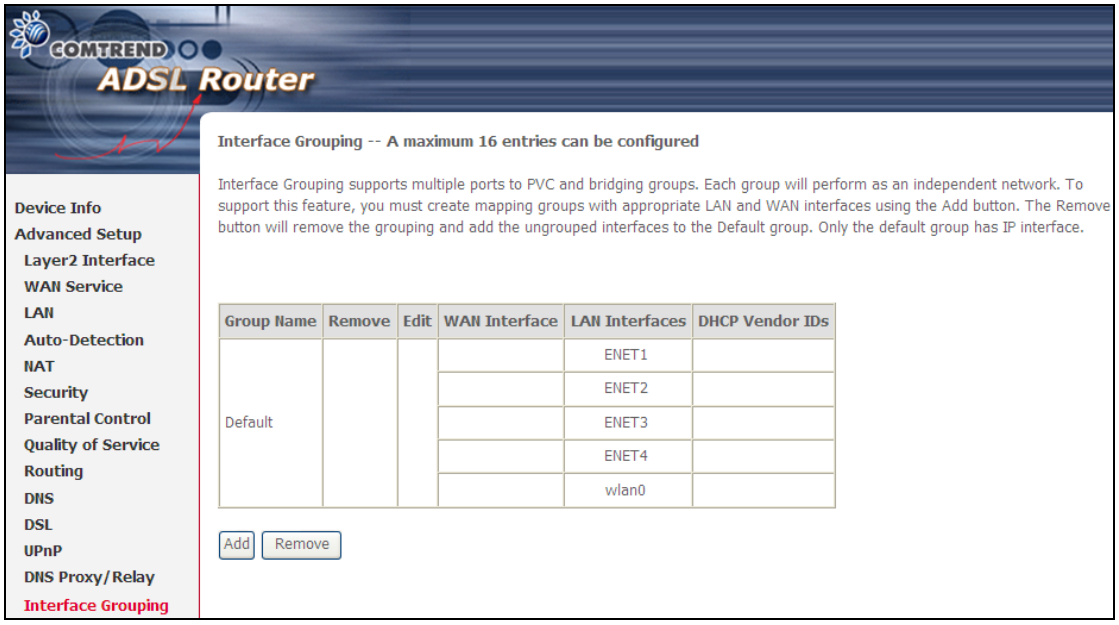


DNS Relay

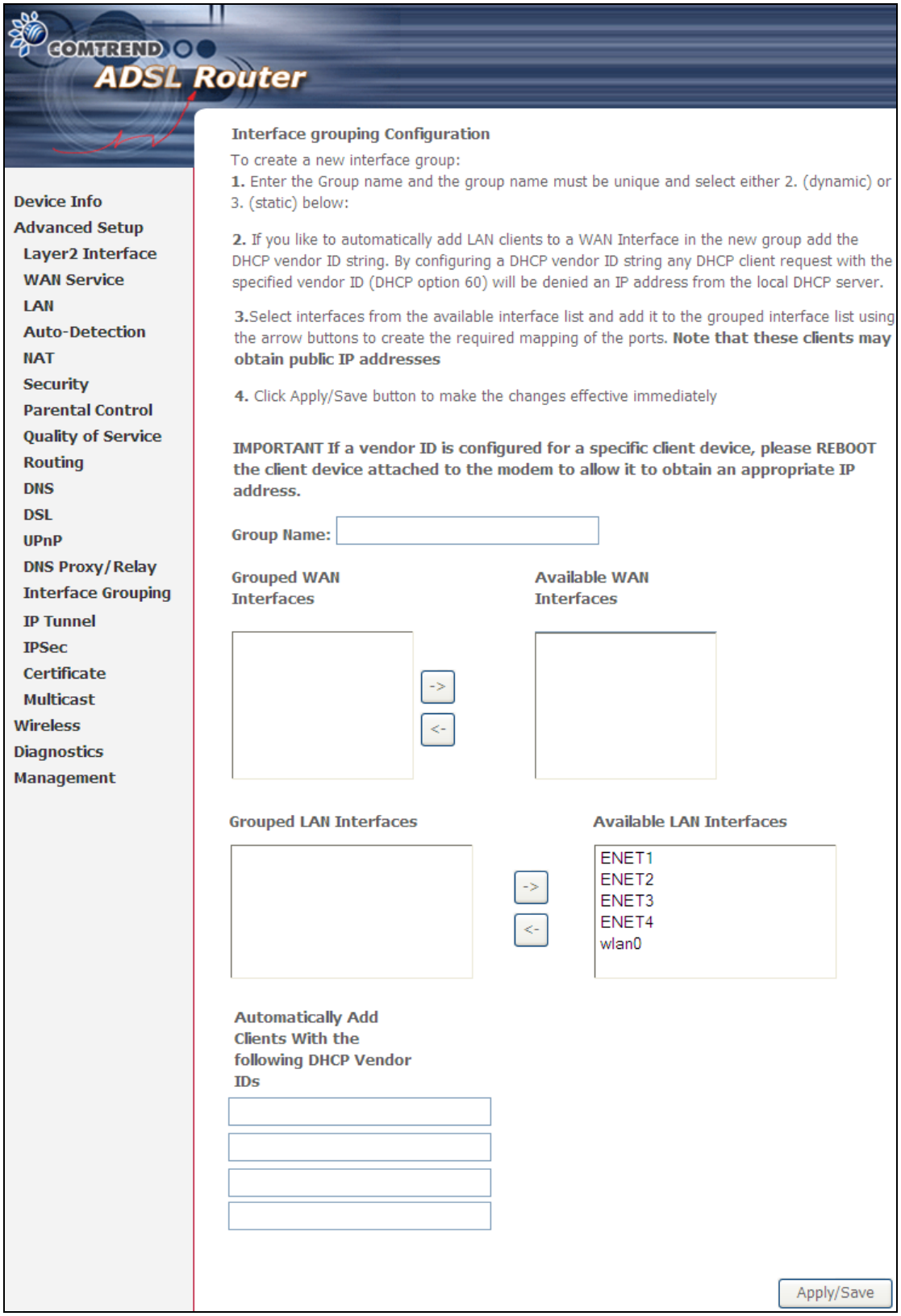
When DNS Relay is enabled, the router will play a role as DNS server that send request to ISP DNS server and cache the information for later access. When DNS relay is disabled, the computer will pull information from ISP DNS server.

5.14 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.
The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.



To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown onscreen.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy/Relay
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Interface grouping Configuration
To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses
4. Click Apply/Save button to make the changes effective immediately
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name:
Grouped WAN Interfaces
Available WAN Interfaces
->
<-
Grouped LAN Interfaces
Available LAN Interfaces
ENET1
ENET2
ENET3
ENET4
wlan0
->
<-
Automatically Add Clients With the following DHCP Vendor IDs
Apply/Save

Automatically Add Clients With Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, and ENET4.

The Interface Grouping configuration will be:

1. Default: ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

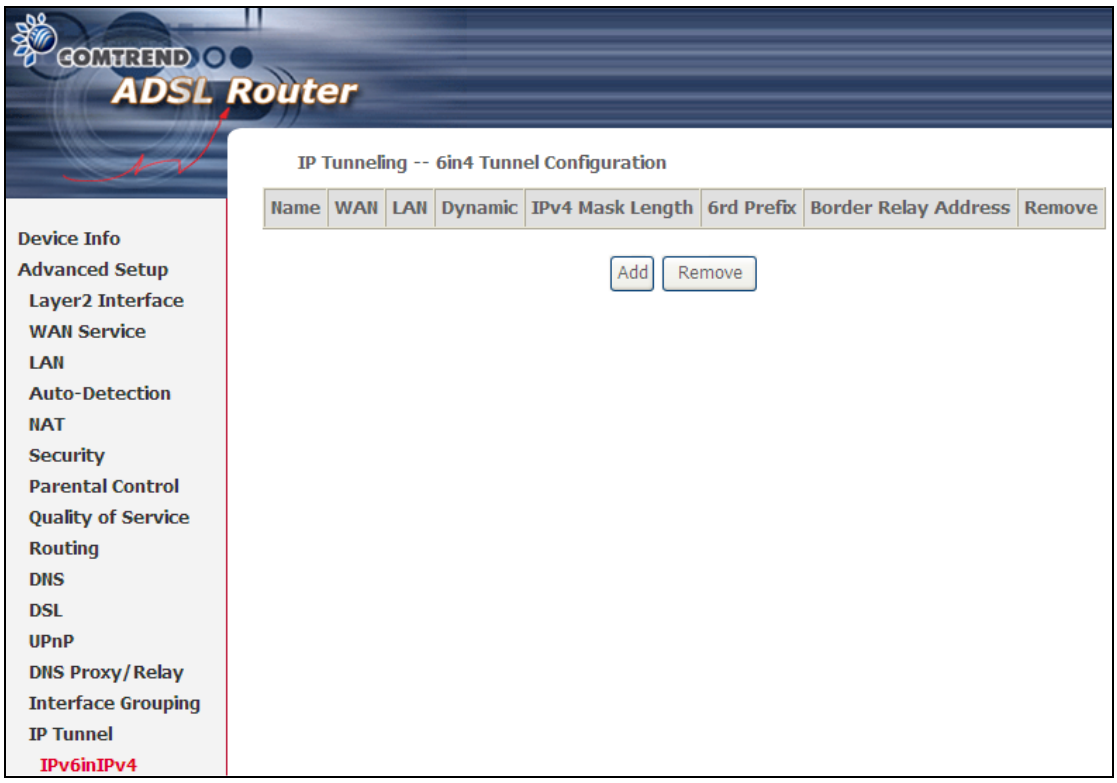
If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ENET2, ENET3, and ENET4
2. Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

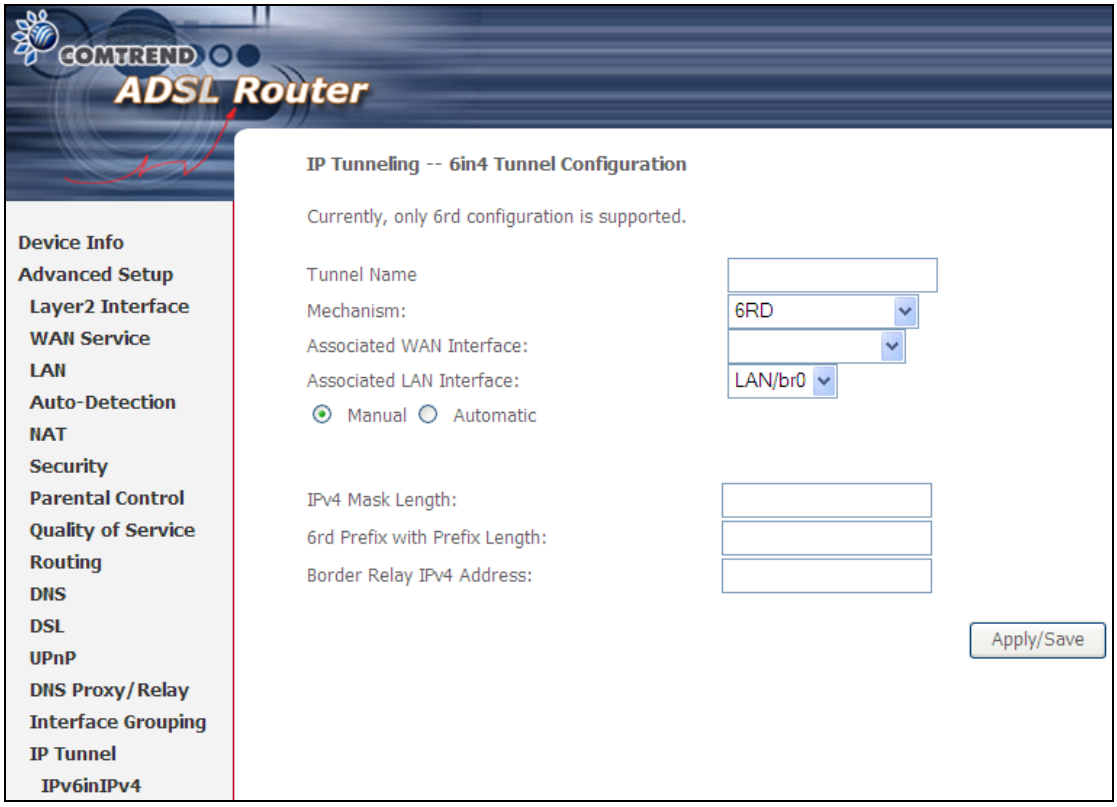
5.15 IP Tunnel

5.15.1 IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.



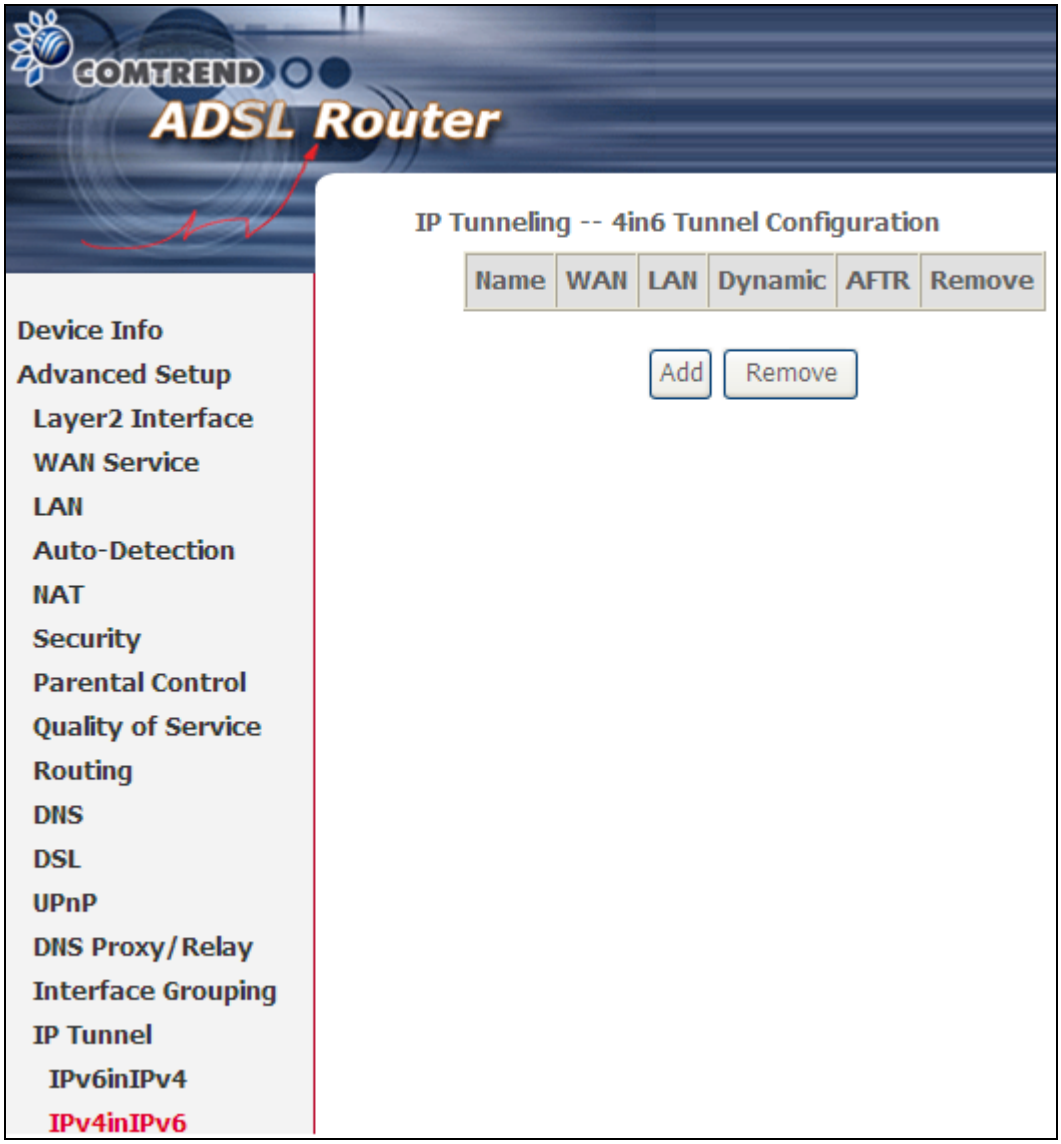
Click the **Add** button to display the following.



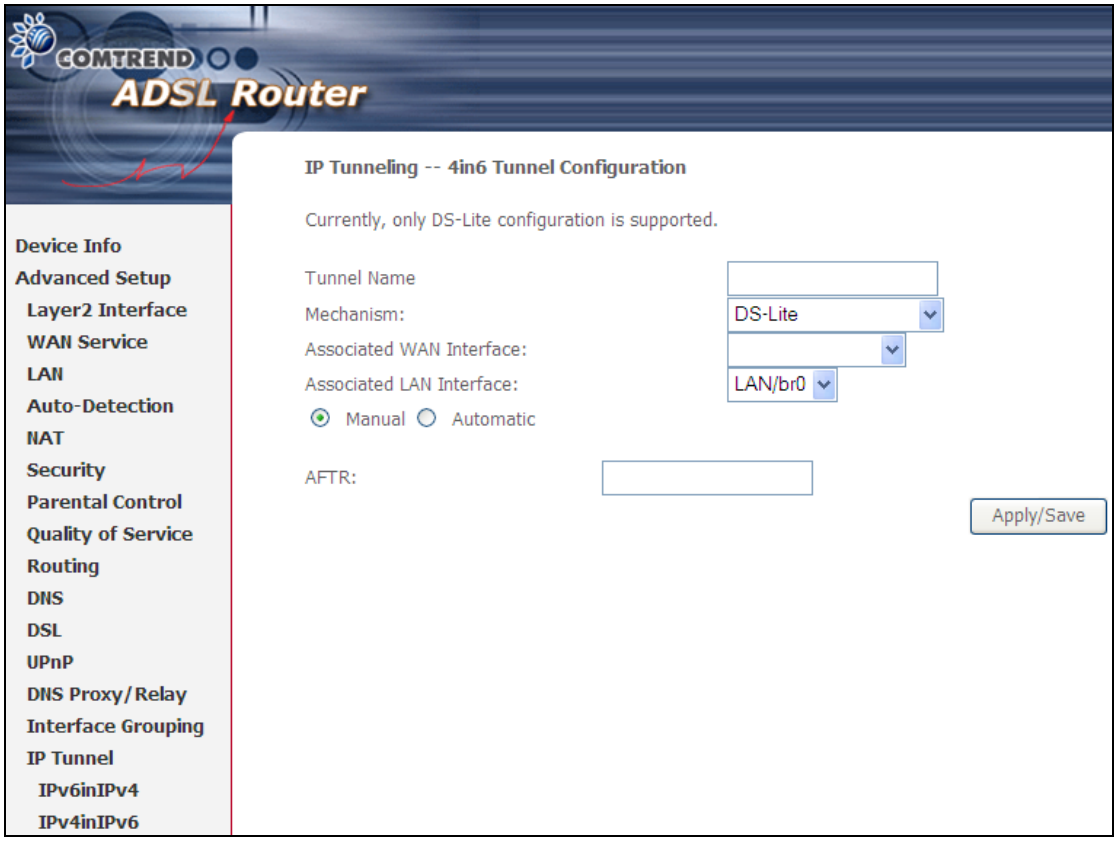
Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used for the IPv4 interface
6rd Prefix with Prefix Length	Prefix and prefix length used for the IPv6 interface
Border Relay IPv4 Address	Input the IPv4 address of the other device

5.15.2 IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.



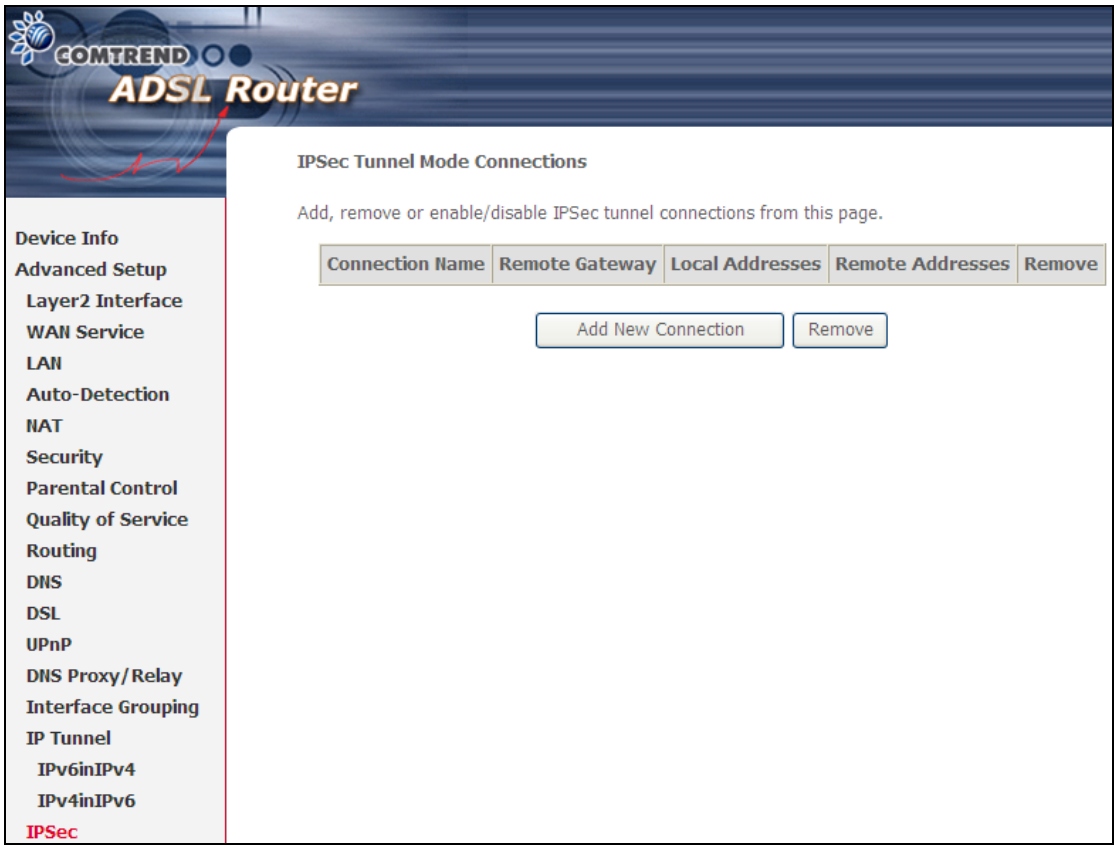
Click the **Add** button to display the following.



Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
AFTR	Address of Address Family Translation Router

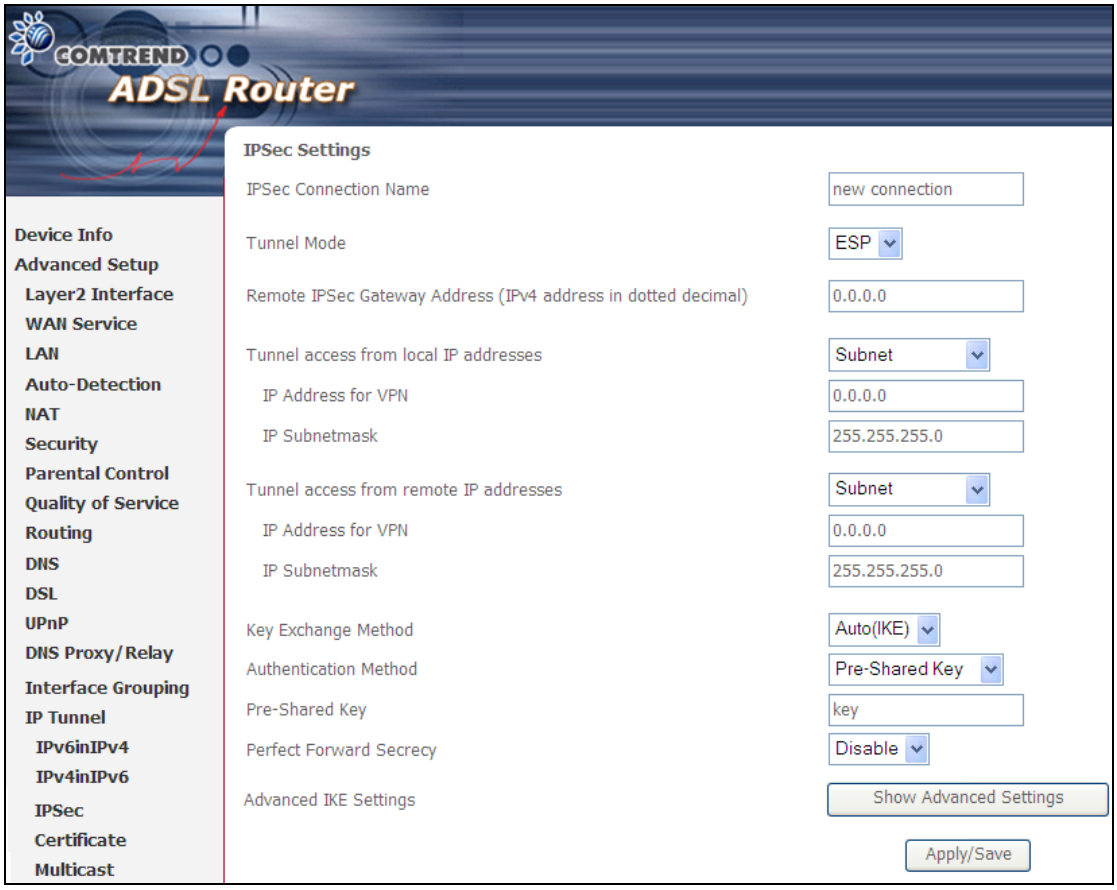
5.16 IPSec

You can add, edit or remove IPSec tunnel mode connections from this page.



Click **Add New Connection** to add a new IPSec termination rule.

The following screen will display.

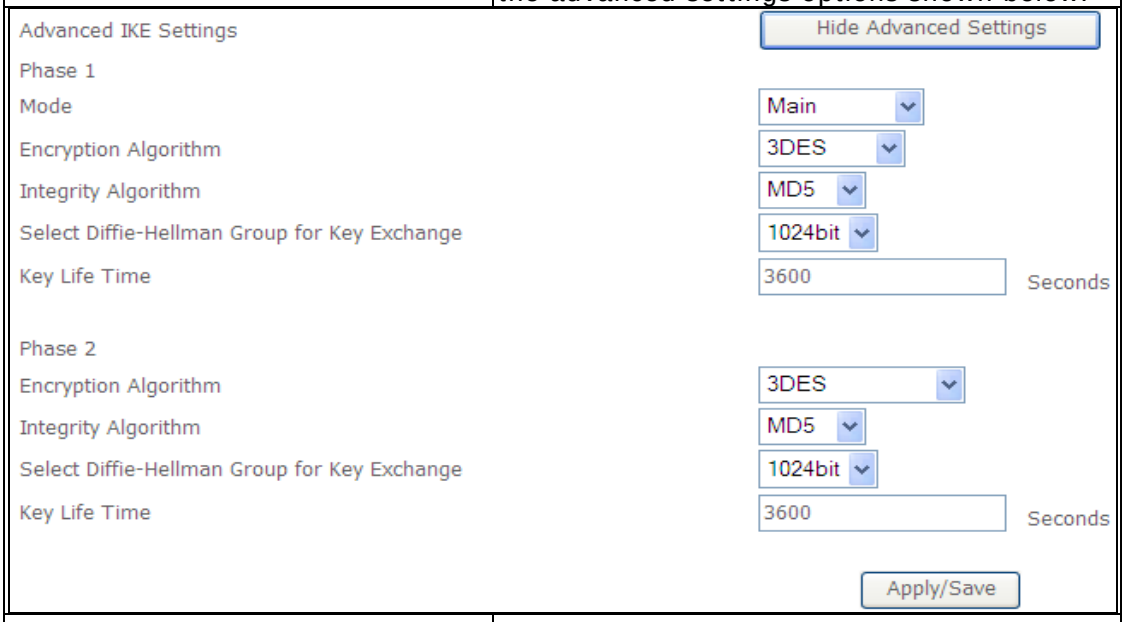


IPSec Connection Name	User-defined label
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

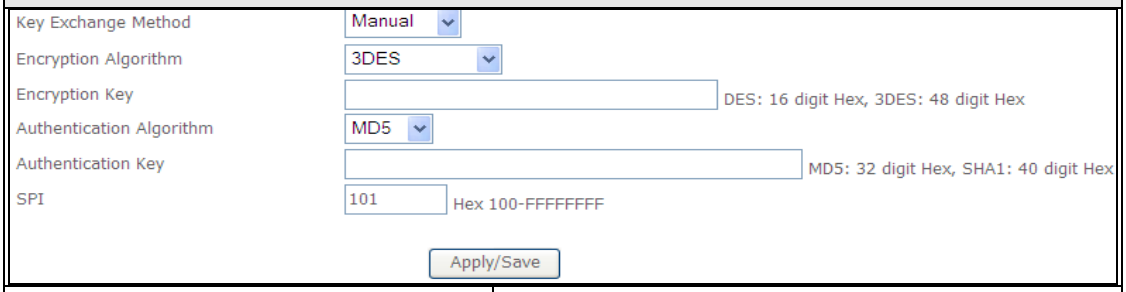
Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.



Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

The Manual key exchange method options are summarized in the table below.

Manual Key Exchange Method	

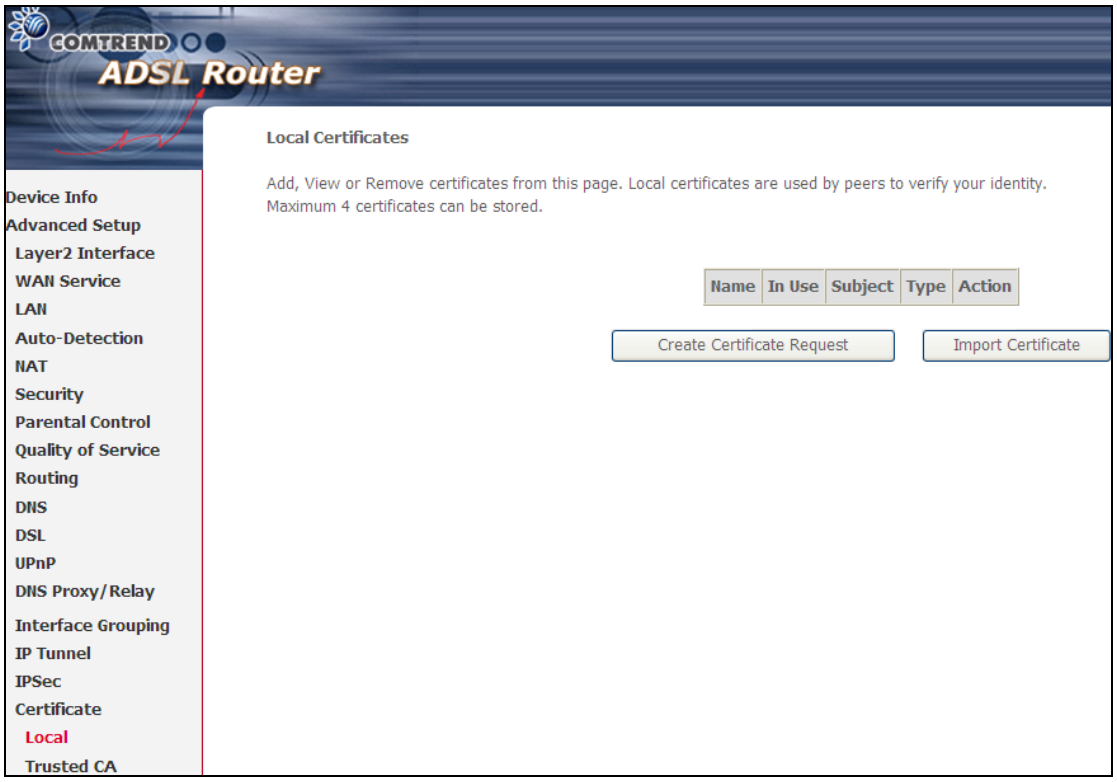


Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

5.17 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

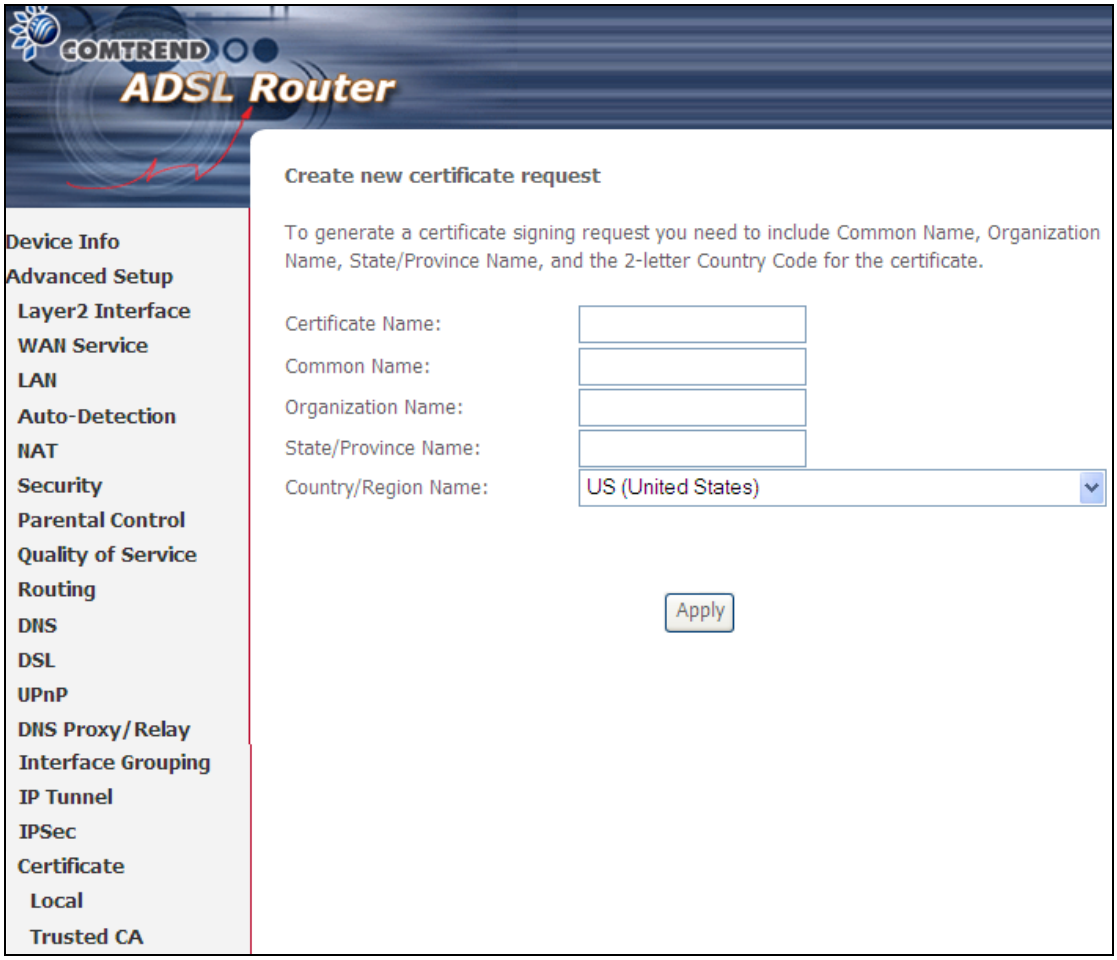
5.17.1 Local



CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.

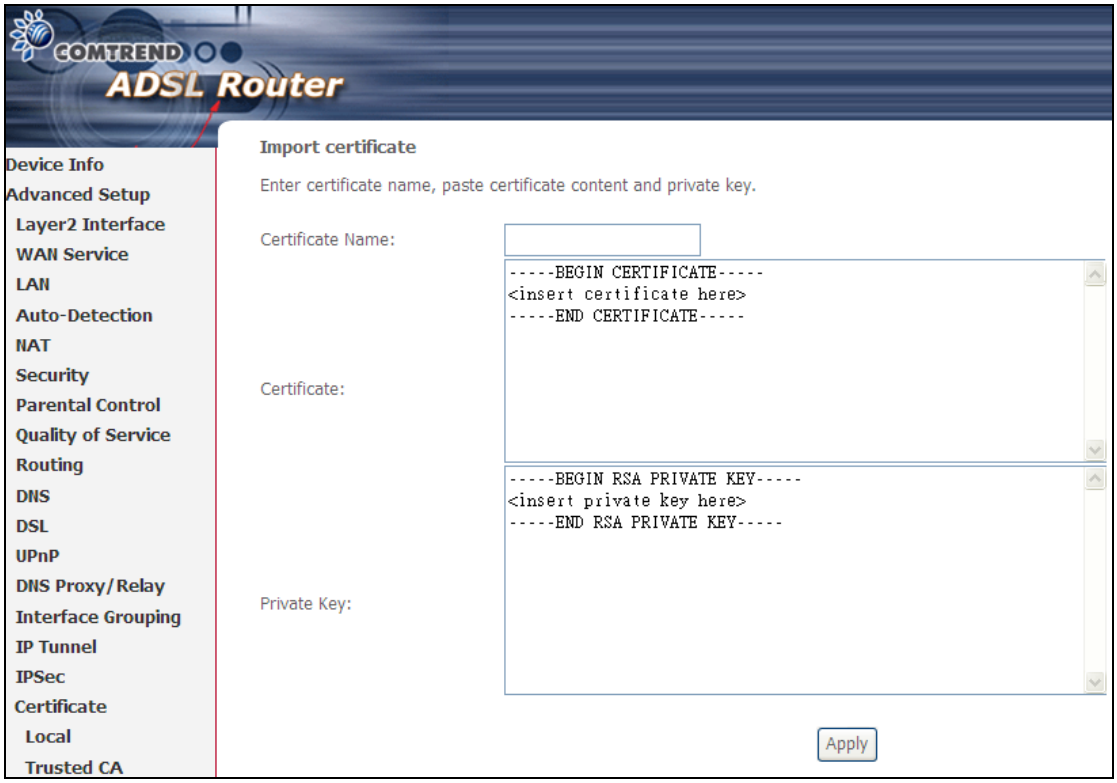


The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

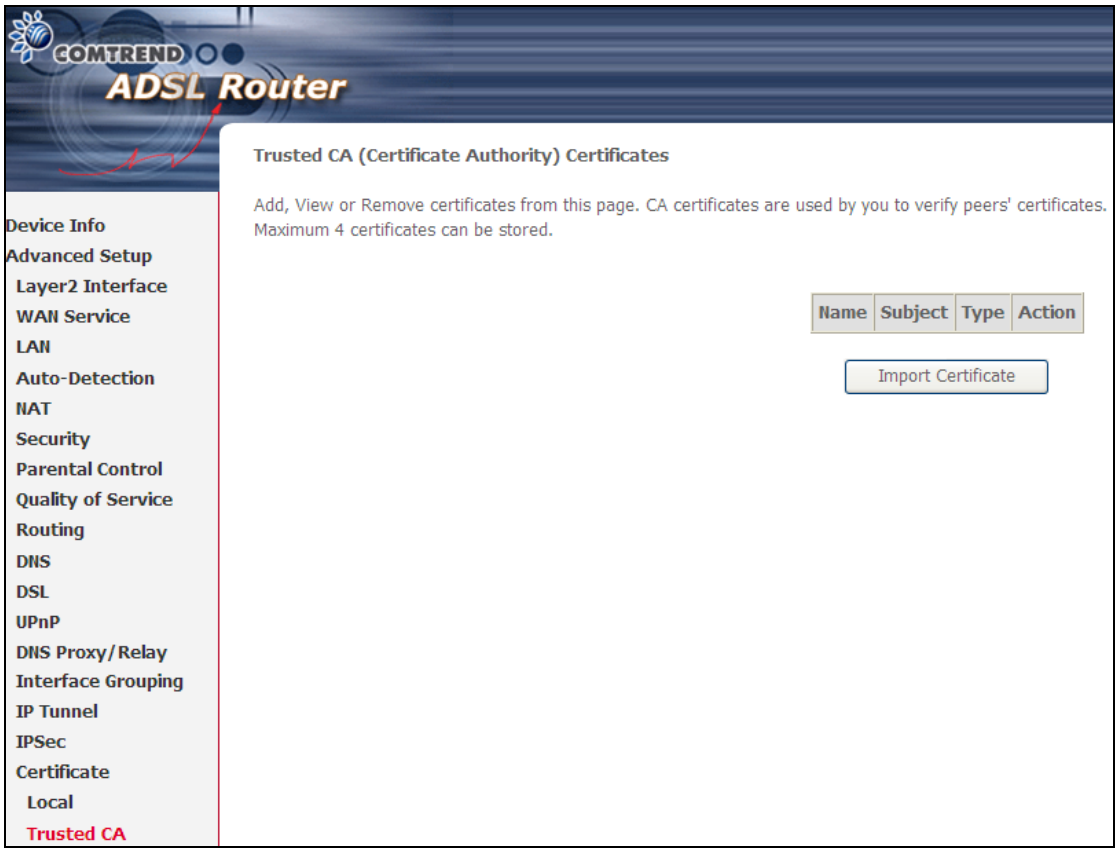
Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.



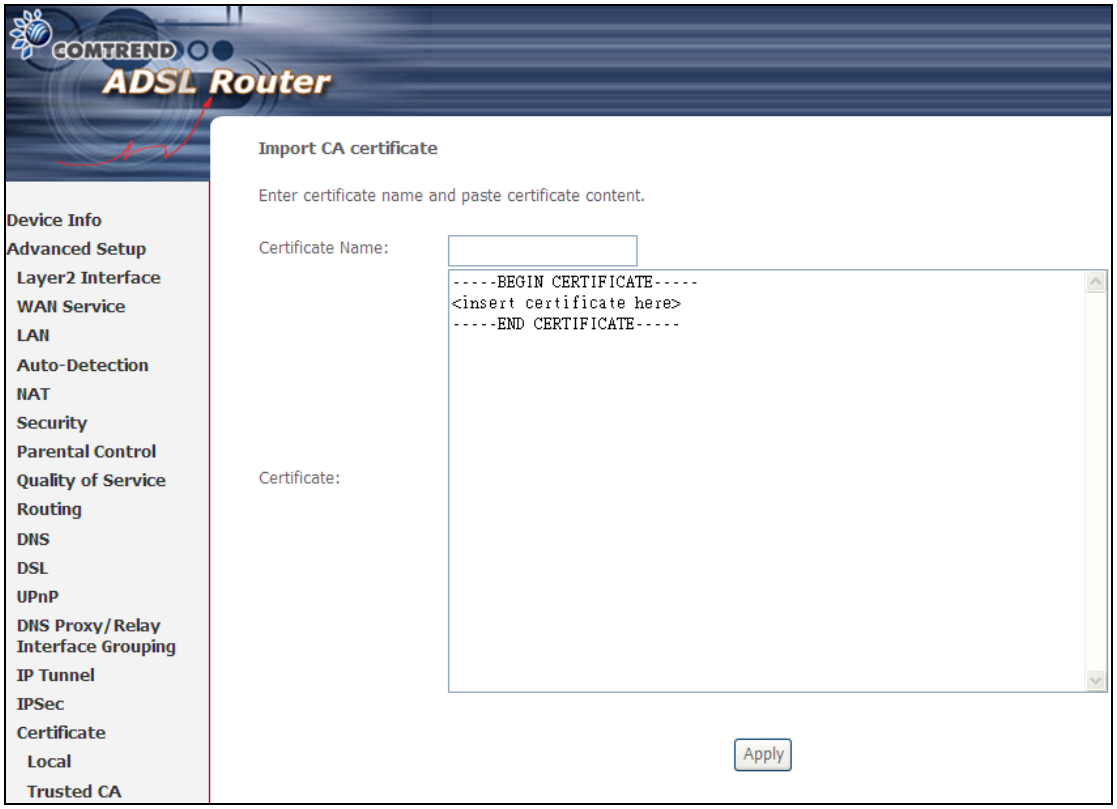
Enter a certificate name and click **Apply** to import the local certificate.

5.17.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.



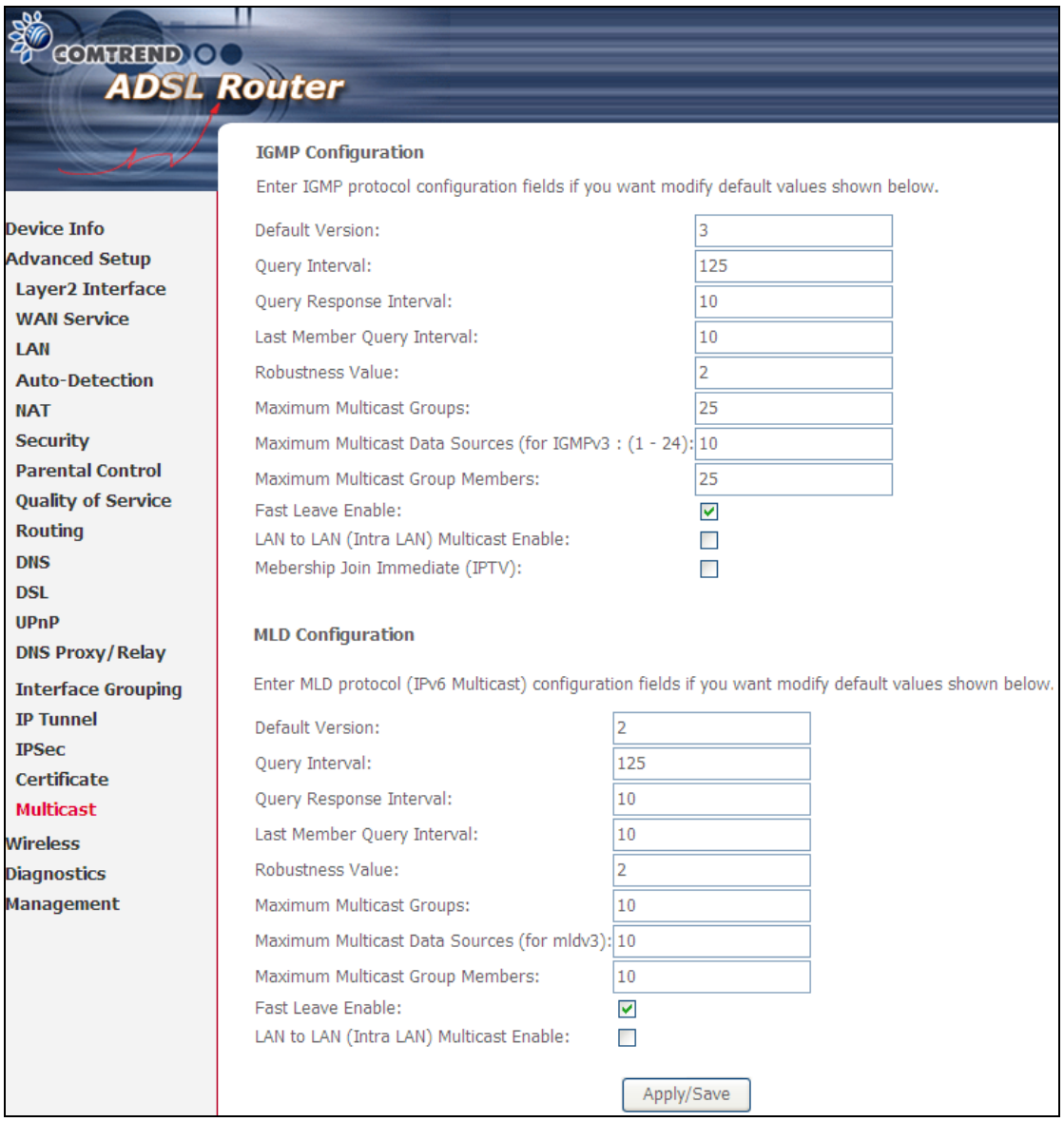
Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Enter a certificate name and click **Apply** to import the CA certificate.

5.18 Multicast

Input new IGMP or MLD protocol configuration fields if you want modify default values shown. Then click **Apply/Save**.



Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.

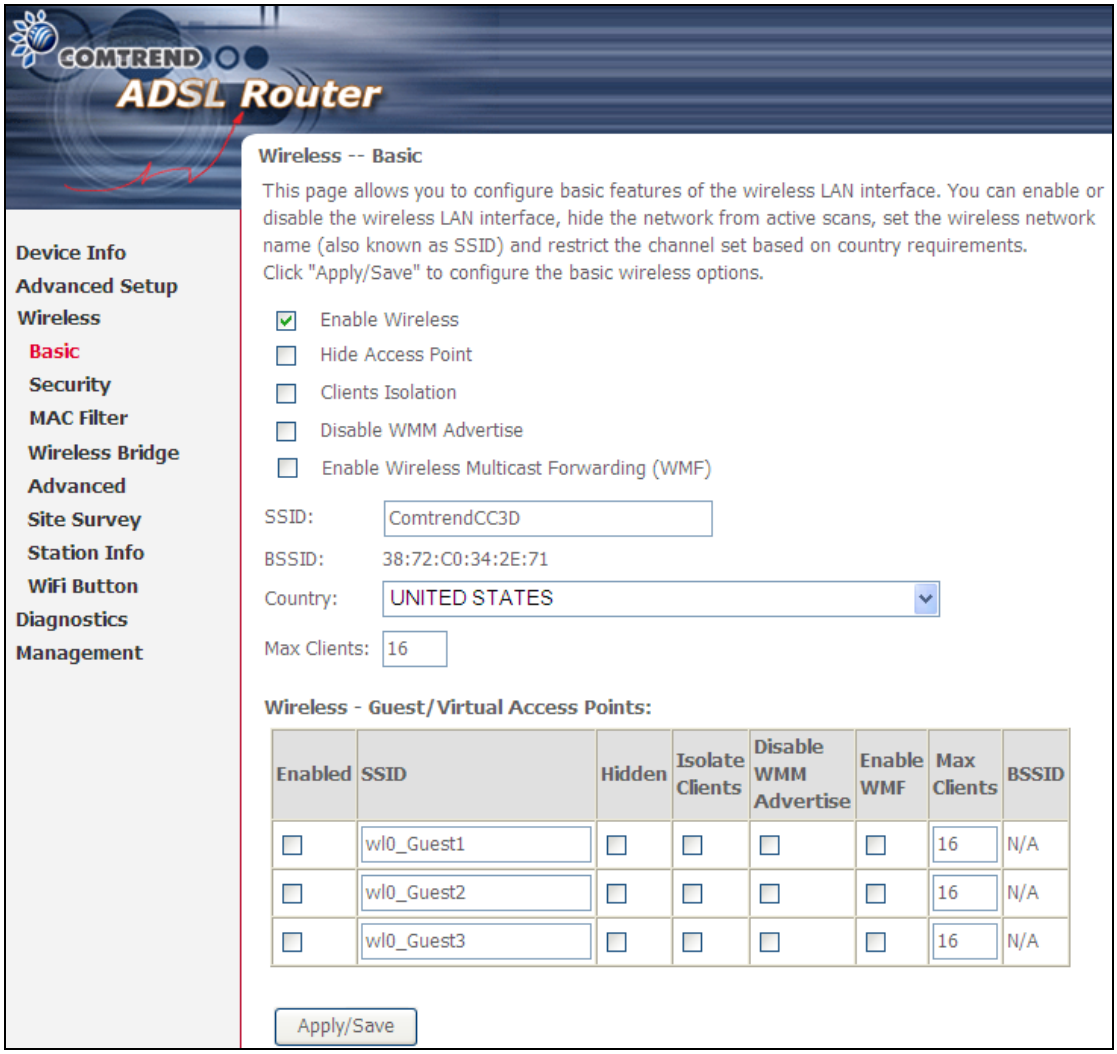
Field	Description
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Last Member Query Interval	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	Setting the maximum number of Multicast groups.
Maximum Multicast Data Sources (for IGMPv3)	Define the maximum multicast video stream number.
Maximum Multicast Group Members	Setting the maximum number of groups that ports can accept.
Fast Leave Enable	When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.
LAN to LAN (Intra LAN) Multicast Enable	This will activate IGMP snooping for cases where multicast data source and player are all located on the LAN side.
Membership to join Immediate (IPTV)	Enable IGMP immediate join feature for multicast membership group.

Chapter 6 Wireless

The Wireless menu provides access to the wireless options discussed below.

6.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Site Survey
Station Info
WiFi Button
Diagnostics
Management
Wireless -- Basic
This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply/Save" to configure the basic wireless options.
Enable Wireless
Hide Access Point
Clients Isolation
Disable WMM Advertise
Enable Wireless Multicast Forwarding (WMF)
SSID: ComtrendCC3D
BSSID: 38:72:C0:34:2E:71
Country: UNITED STATES
Max Clients: 16
Wireless - Guest/Virtual Access Points:
Enabled SSID Hidden Isolate Clients Disable WMM Advertise Enable WMF Max Clients BSSID
wl0_Guest1 16 N/A
wl0_Guest2 16 N/A
wl0_Guest3 16 N/A
Apply/Save

Click **Apply / Save** to apply the selected wireless options.

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Select the checkbox ☑ to enable this function.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Enable WMF**, **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

6.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.

Click **Apply / Save** to implement new configuration settings.

WIRELESS SECURITY

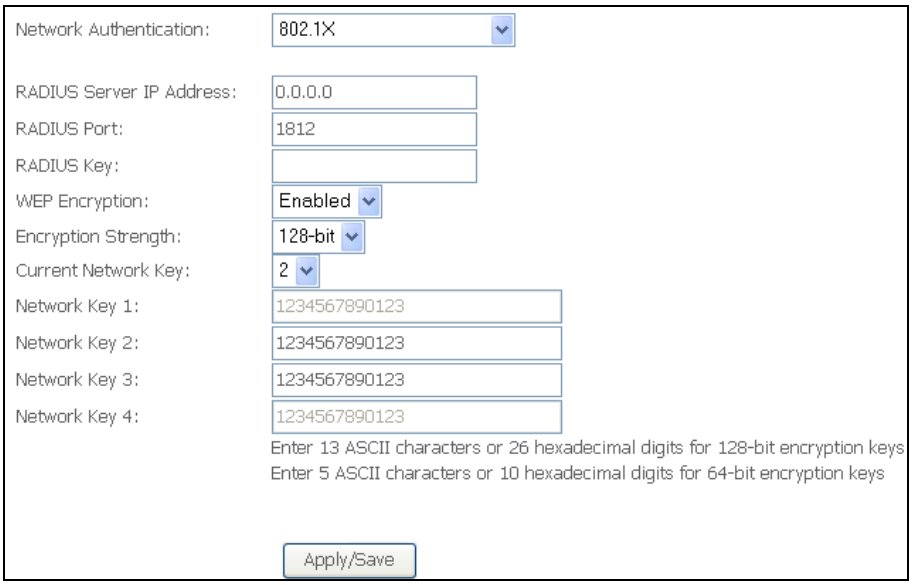
Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see 6.2.1 WPS) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

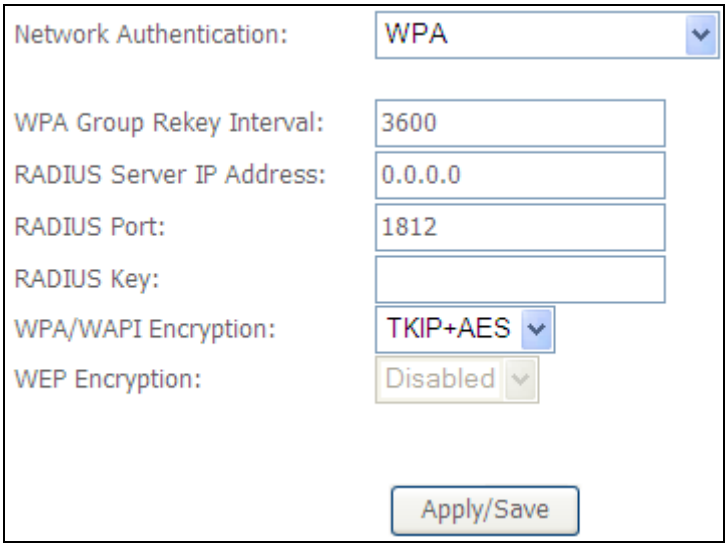
Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

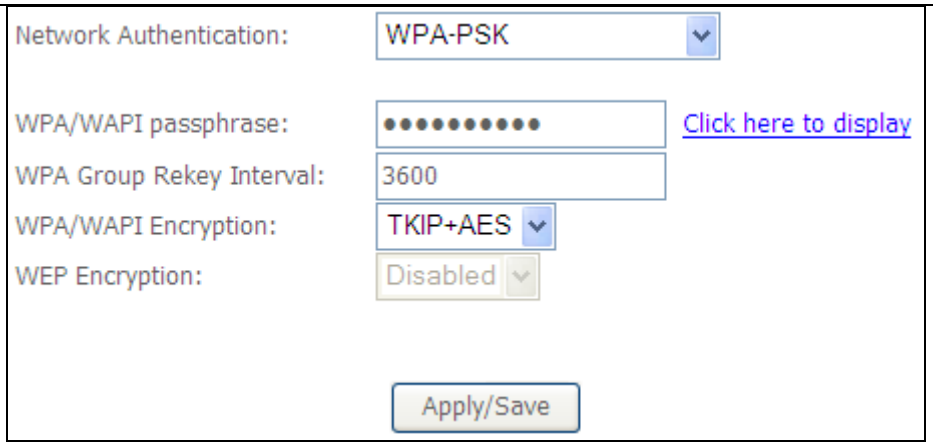
Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.


Network Authentication: 802.1X
RADIUS Server IP Address: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:
WEP Encryption: Enabled
Encryption Strength: 128-bit
Current Network Key: 2
Network Key 1: 1234567890123
Network Key 2: 1234567890123
Network Key 3: 1234567890123
Network Key 4: 1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
Apply/Save

The settings for WPA authentication are shown below.



The settings for WPA-PSK authentication are shown next.



WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has a PIN number accessed through device software. The AR-5389u has a virtual button accessible from the web user interface (WUI).

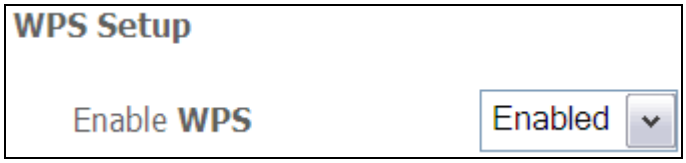
Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".

NOTE:	WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

I. Setup

Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.

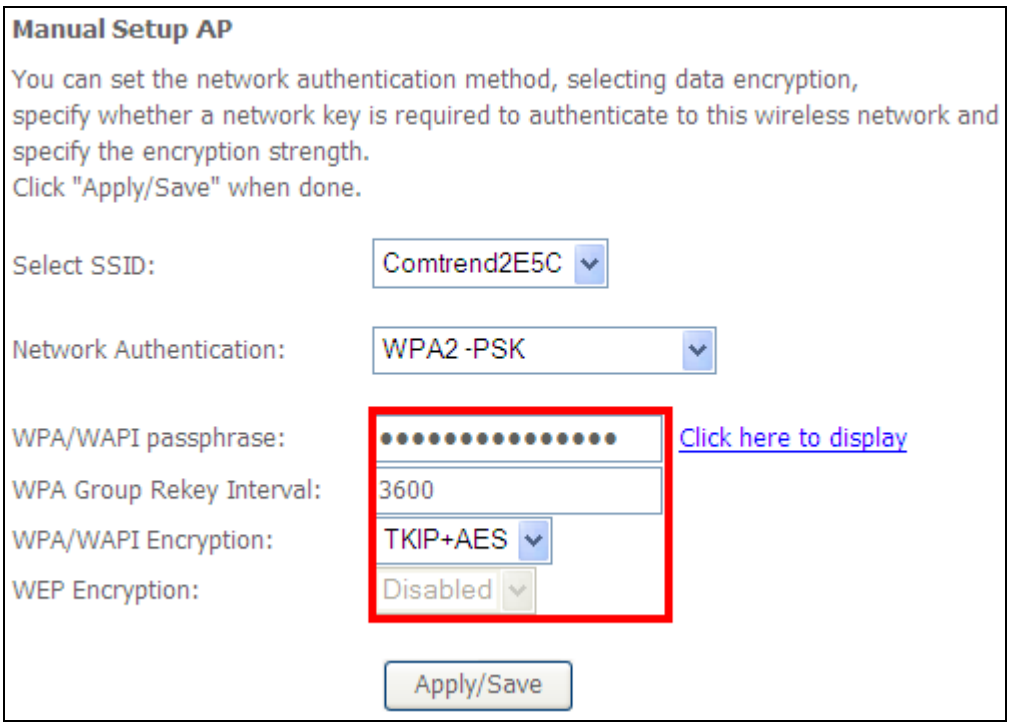


Step 2: Set the WPS AP Mode. **Configured** is used when the AR-5389 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the AR-5389.

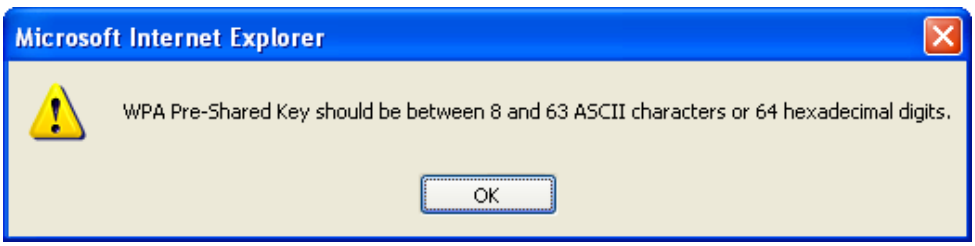
NOTES:	Your client may or may not have the ability to provide security settings to the AR-5389. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities. In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button (Appendix D - WPS OPERATION) has detailed instructions).

II. NETWORK AUTHENTICATION

Step 3: Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.



Step 4: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You will see the following dialog box if the Key is too short or too long.



Step 5: Click the **Apply / Save** button at the bottom of the screen.

III a. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

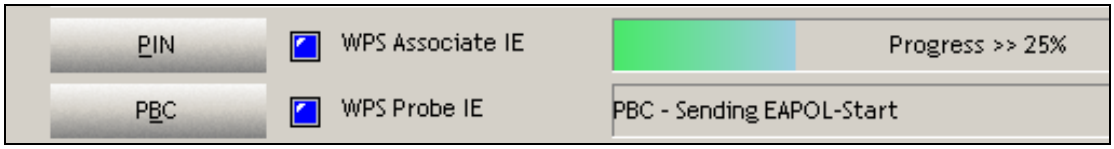
The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

Step 6: Press WPS button

Press the WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Step 7: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IIIb. WPS – PIN CONFIGURATION

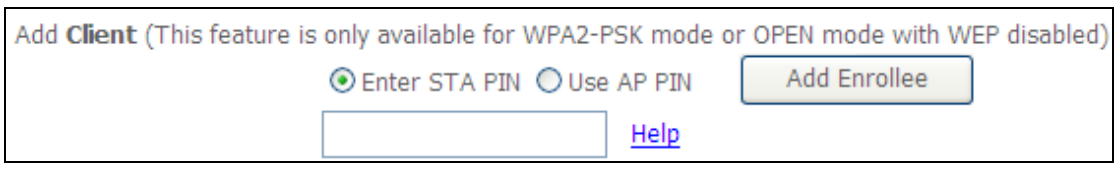
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

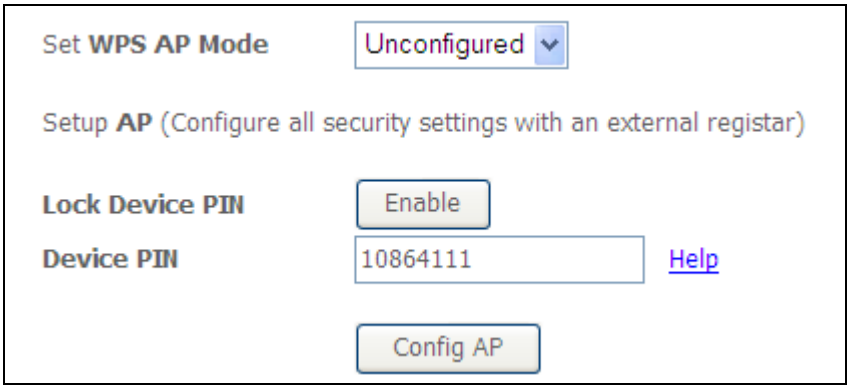
Step 6: Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

A - For **Configured** mode, click the **Add Enrollee** button.


Add Client (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)
Enter STA PIN
Use AP PIN
Add Enrollee
Help

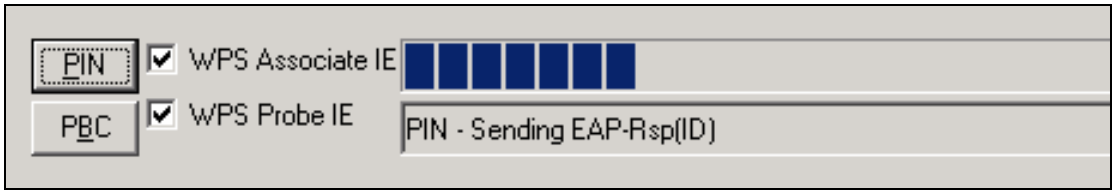
Enter STA PIN: a Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be inputted at representing the network, usually the Access Point of the network.

B - For **Unconfigured** mode, click the **Config AP** button.



Step 7: Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

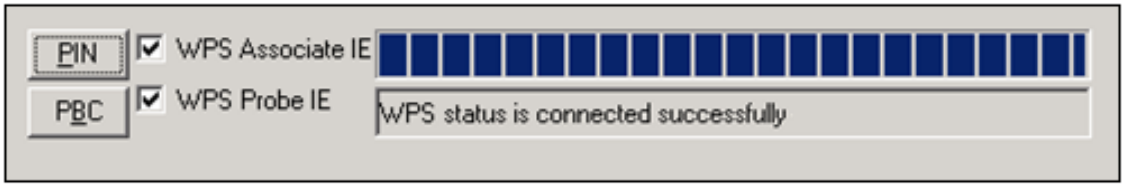
The figure below provides an example of a WPS client PIN function in-progress.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IV. CHECK CONNECTION

Step 8: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

6.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.

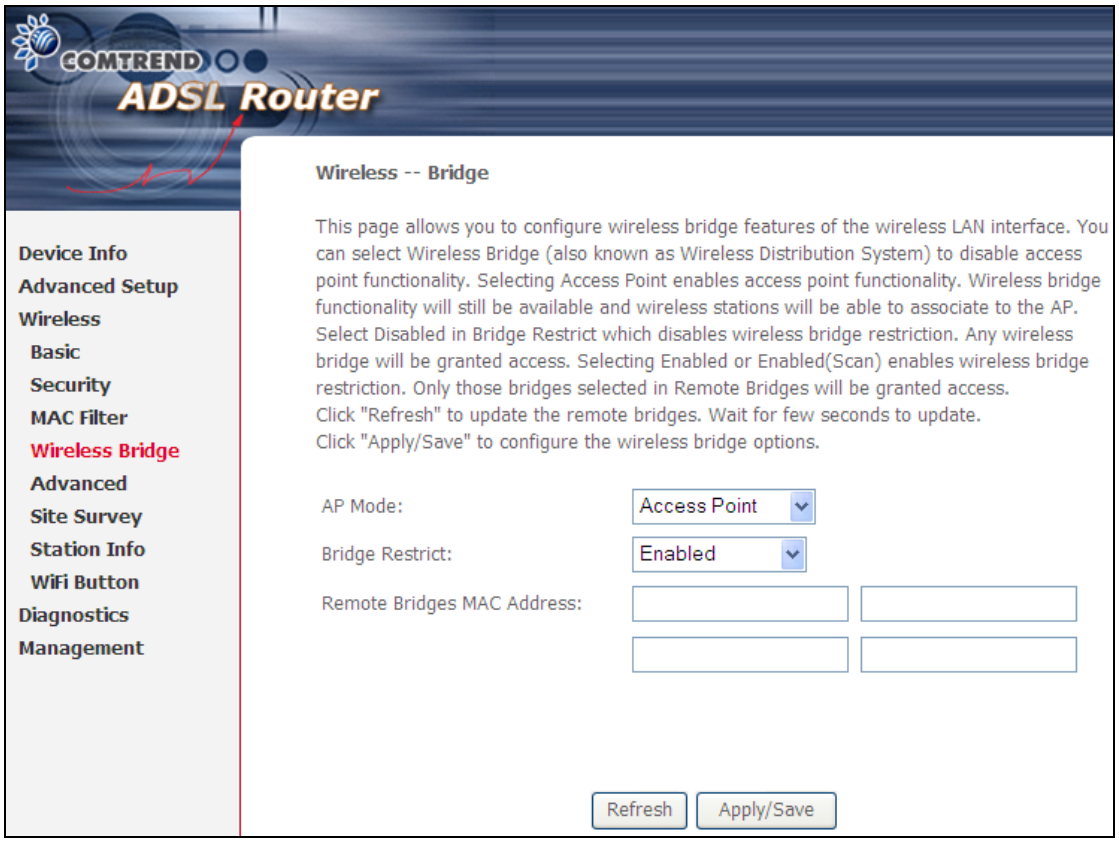
Option	Description
Select SSID	Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.

Enter the MAC address in the box provided and click **Apply/Save.**

6.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WIFI interface. See the table beneath for detailed explanations of the various options.

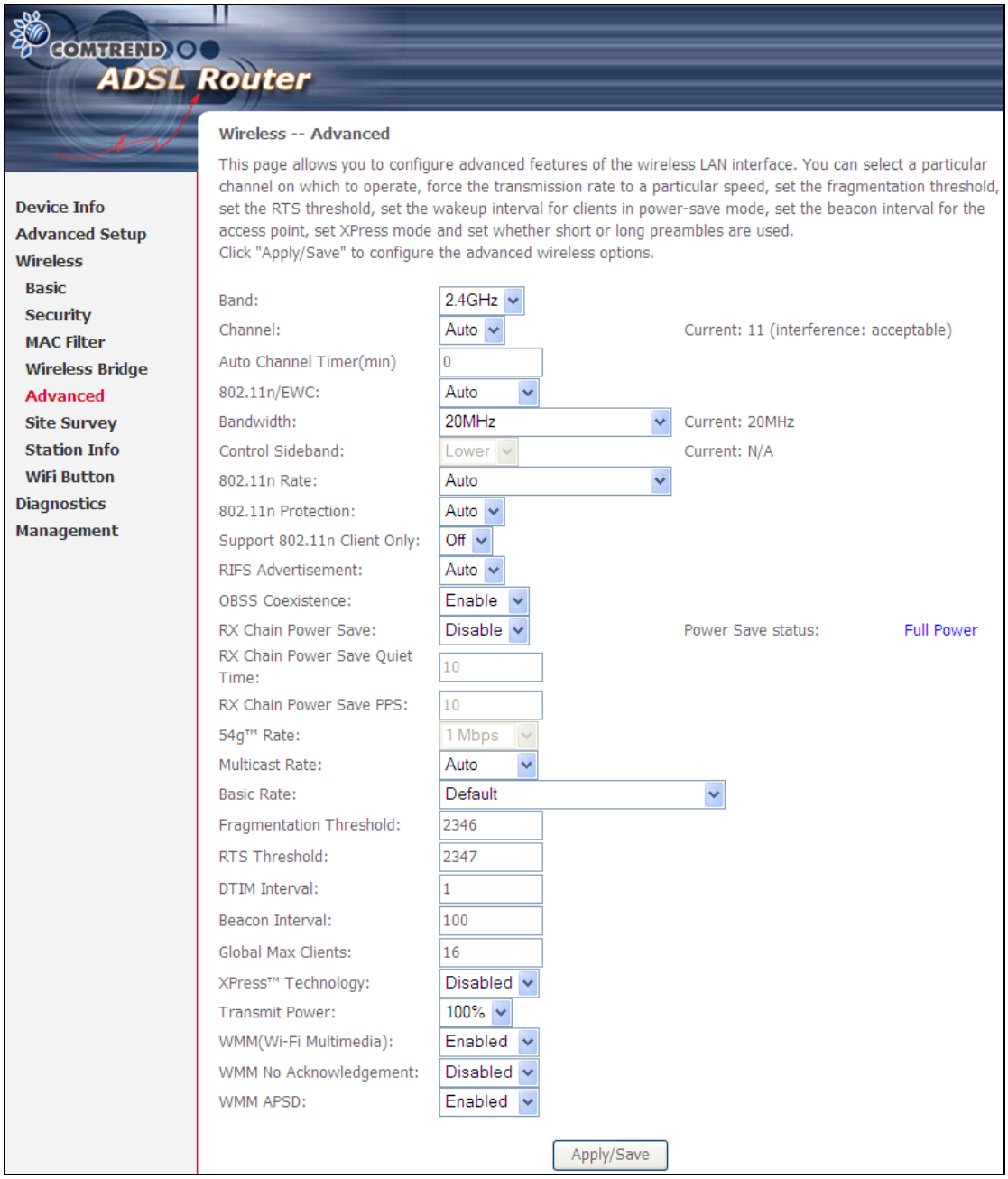

COMTREND
ADSL Router
Wireless -- Bridge
This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Site Survey
Station Info
WiFi Button
Diagnostics
Management
AP Mode:
Access Point
Bridge Restrict:
Enabled
Remote Bridges MAC Address:
Refresh
Apply/Save

Click **Apply/Save** to implement new configuration settings.

Feature	Description
AP Mode	Selecting **Wireless Bridge** (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting **Access Point** enables AP functionality. In **Access Point** mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting **Disabled** disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click **Refresh** to update the station list when Bridge Restrict is enabled.

6.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Apply / Save** to set new advanced wireless options.

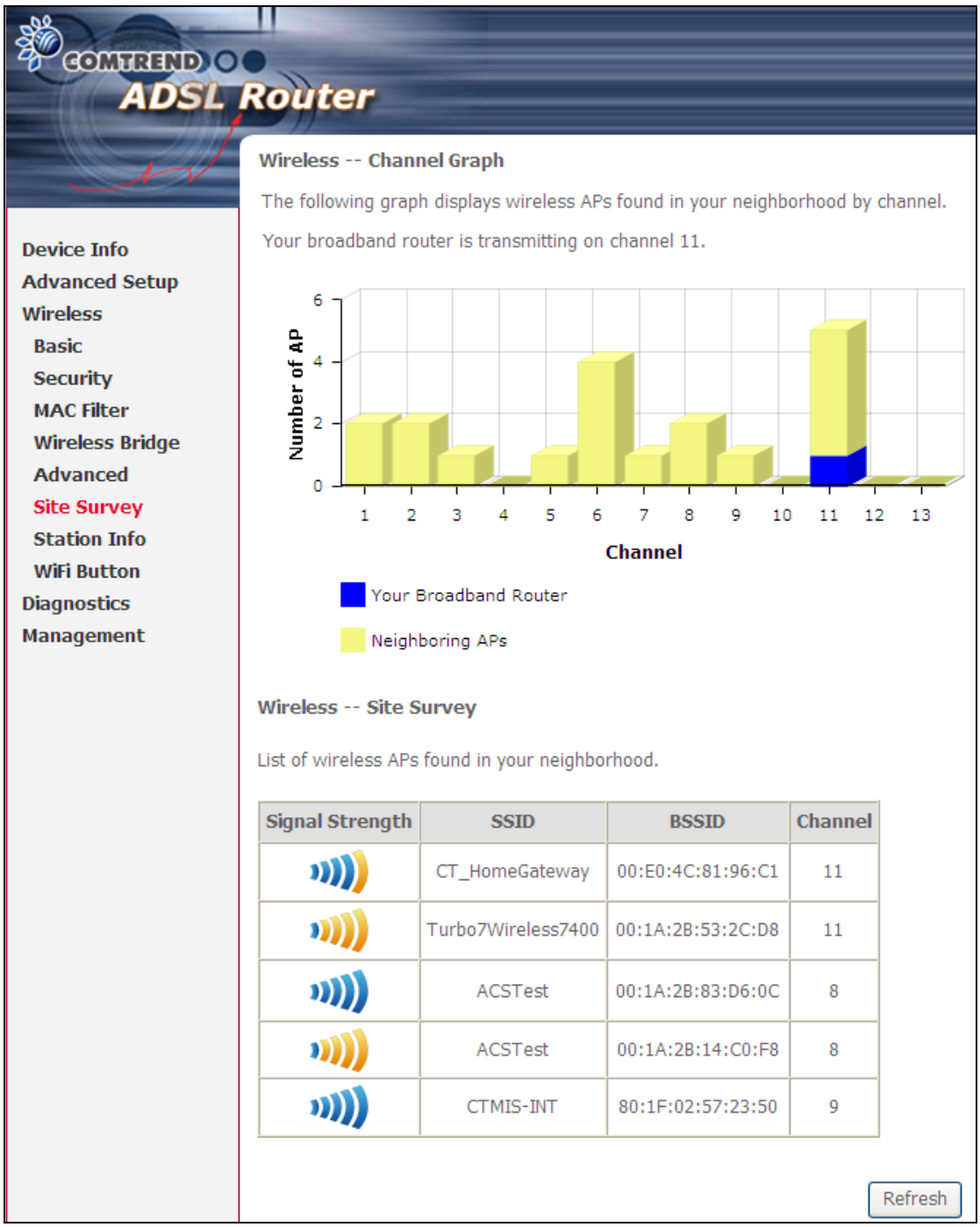

COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Site Survey
Station Info
WiFi Button
Diagnostics
Management
Wireless -- Advanced
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply/Save" to configure the advanced wireless options.
Band: 2.4GHz
Channel: Auto Current: 11 (interference: acceptable)
Auto Channel Timer(min) 0
802.11n/EWC: Auto
Bandwidth: 20MHz Current: 20MHz
Control Sideband: Lower Current: N/A
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
RIFS Advertisement: Auto
OBSS Coexistence: Enable
RX Chain Power Save: Disable Power Save status: Full Power
RX Chain Power Save Quiet Time: 10
RX Chain Power Save PPS: 10
54g™ Rate: 1 Mbps
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 16
XPress™ Technology: Disabled
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enabled
WMM No Acknowledgement: Disabled
WMM APSD: Enabled
Apply/Save

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20MHz or 40MHz bandwidth. 40MHz bandwidth uses two adjacent 20MHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40MHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients' access to the router.
RIFS Advertisement	One of several draft-n features designed to improve efficiency. Provides a shorter delay between OFDM transmissions than in802.11a or g.
OBSS Co-Existence	Co-existence between 20 MHZ AND 40 MHZ overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.

Field	Description
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

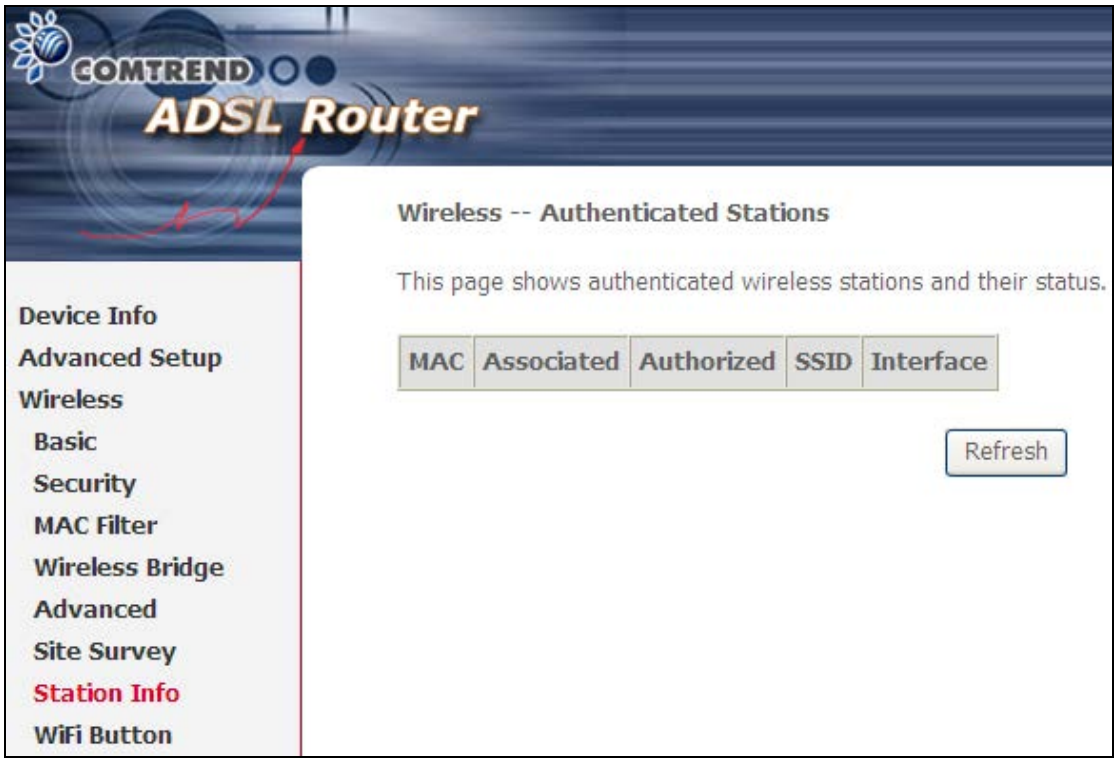
6.6 Site Survey

The graph displays wireless APs found in your neighborhood by channel.



6.7 Station Info

This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.

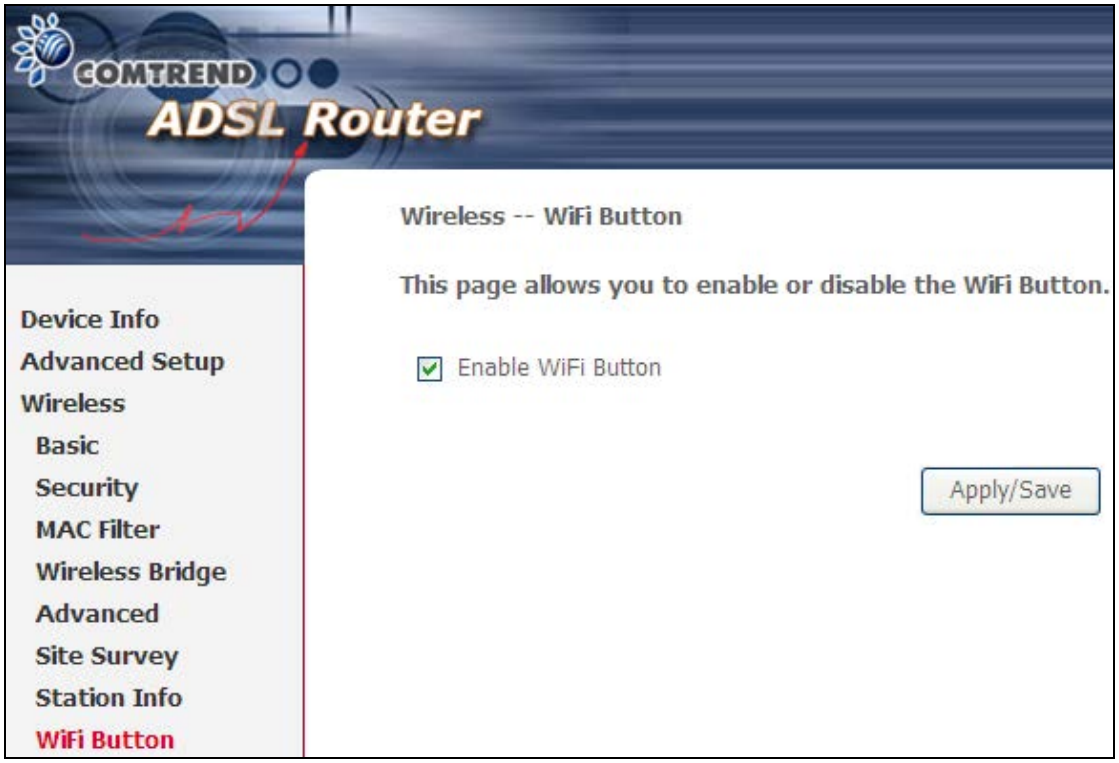


Consult the table below for descriptions of each column heading.

Heading	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

6.8 WiFi Button

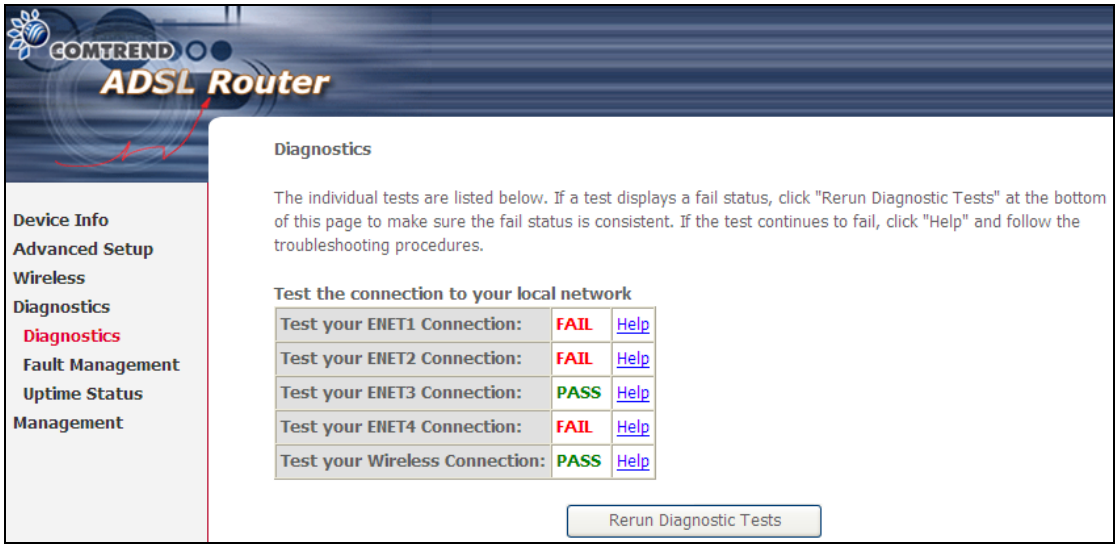
This page allows you to enable or disable the WiFi Button.



Chapter 7 Diagnostics

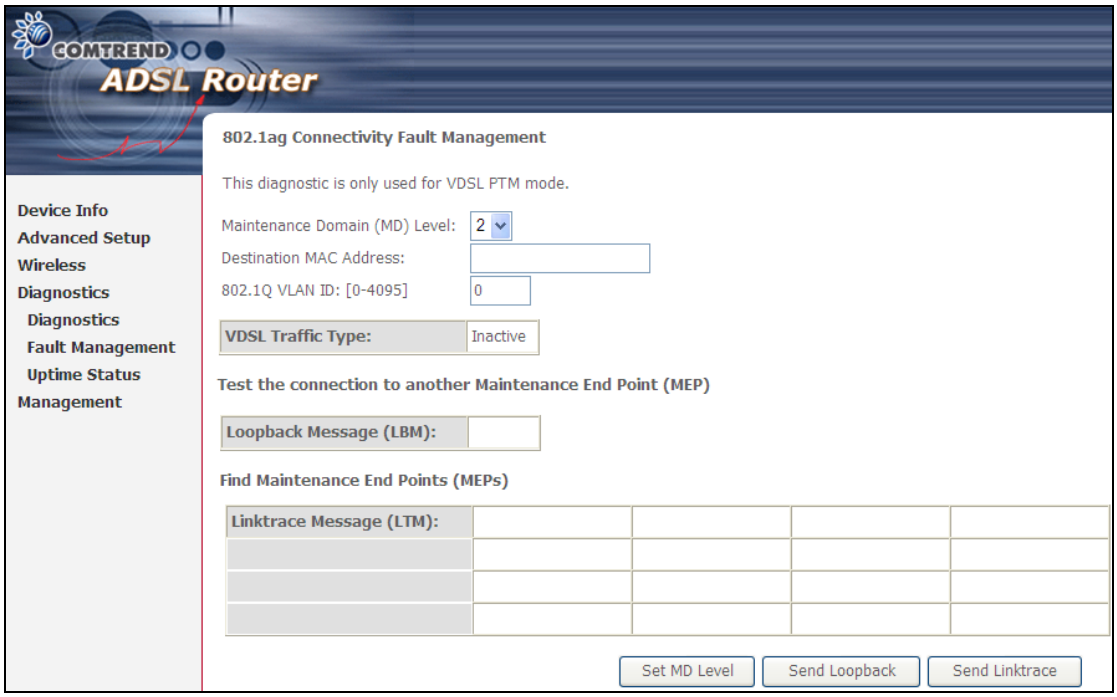
7.1 Diagnostics – Individual Tests

The first Diagnostics screen is a dashboard that shows overall connection status.
If a test displays a fail status, click the button to retest and confirm the error.
If a test continues to fail, click Help and follow the troubleshooting procedures.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Diagnostics
Fault Management
Uptime Status
Management
Diagnostics
The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET1 Connection: FAIL Help
Test your ENET2 Connection: FAIL Help
Test your ENET3 Connection: PASS Help
Test your ENET4 Connection: FAIL Help
Test your Wireless Connection: PASS Help
Rerun Diagnostic Tests

7.2 Fault Management

The second Diagnostics screen (Fault Management) is used for VDSL diagnostics.



Item	Description
Maintenance Domain (MD) Level	Management space on the network, the larger the domain, the higher the level value
Destination MAC Address	Destination MAC address for sending the loopback message
802.1Q VLAN ID: [0-4095]	802.1Q VLAN used in VDSL PTM mode

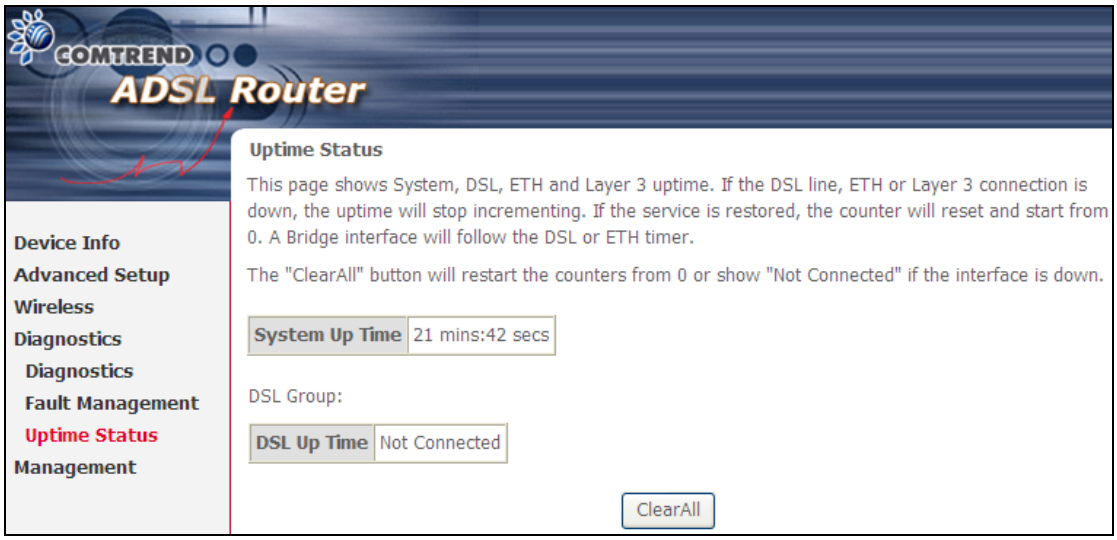
Set MD Level
Save the Maintenance domain level.

Send Loopback
Send loopback message to destination MAC address.

Send Linktrace
Send traceroute message to destination MAC address.

7.3 Uptime Status

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Diagnostics
Fault Management
Uptime Status
Management
Uptime Status
This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.
The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.
System Up Time
21 mins:42 secs
DSL Group:
DSL Up Time
Not Connected
ClearAll

The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.

Chapter 8 Management

Click on the link to jump to a specific section:

8.1 Settings

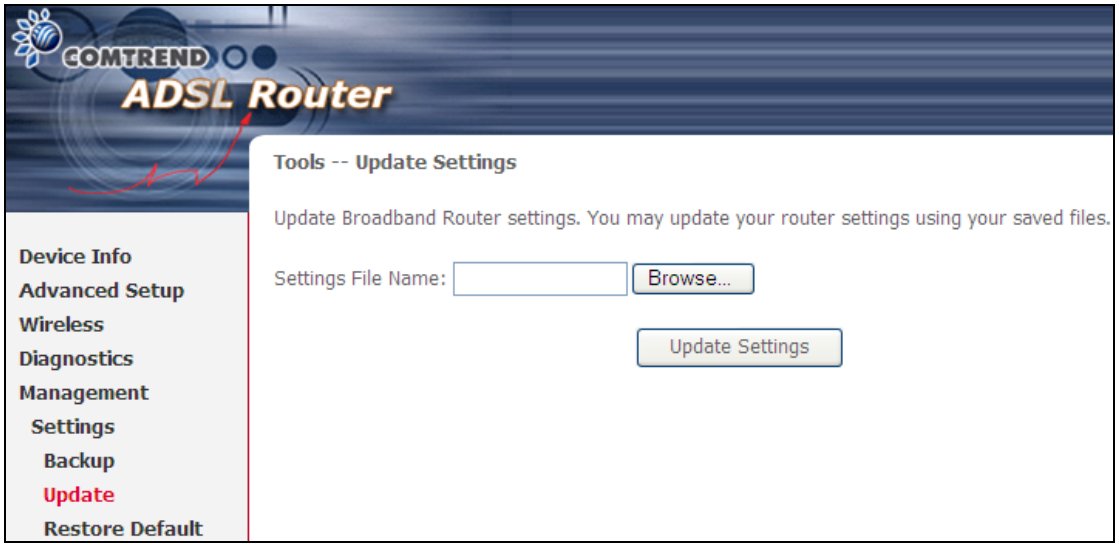
This includes 8.1.1 Backup Settings, 8.1.2 Update Settings, and 8.1.3 Restore Default screens.

8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.

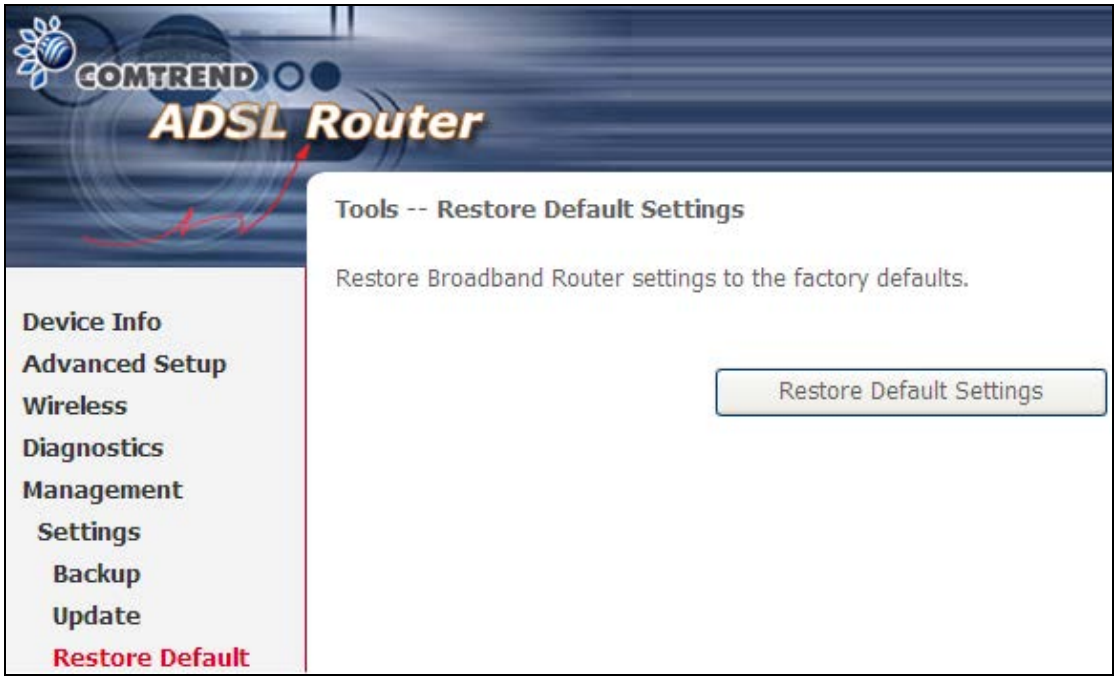
8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse…** to search for the file, then click **Update Settings** to recover settings.

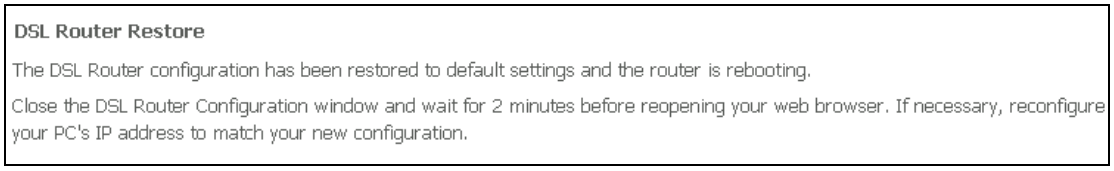


8.1.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.



After **Restore Default Settings** is clicked, the following screen appears.


DSL Router Restore
The DSL Router configuration has been restored to default settings and the router is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

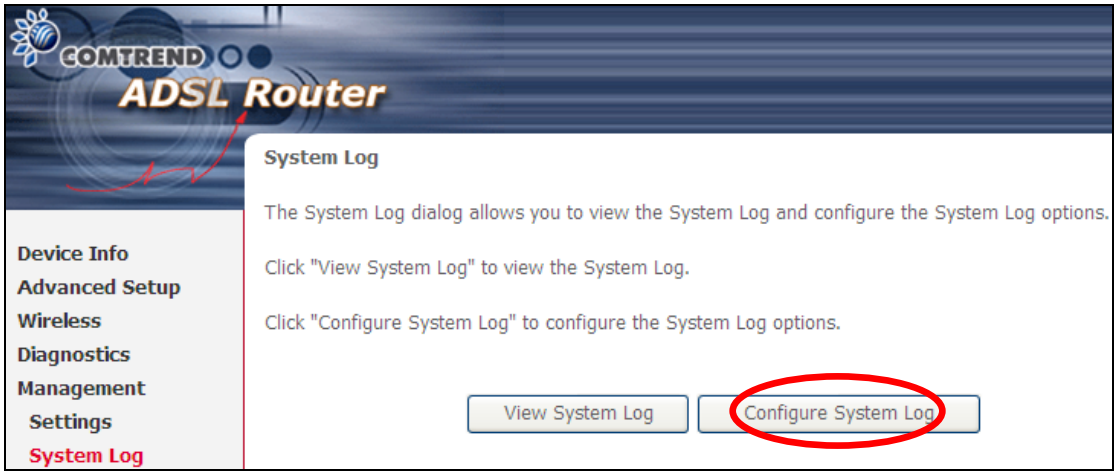
NOTE:	This entry has the same effect as the **Reset** button. The AR-5389 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase the configuration data saved in flash memory.

8.2 System Log

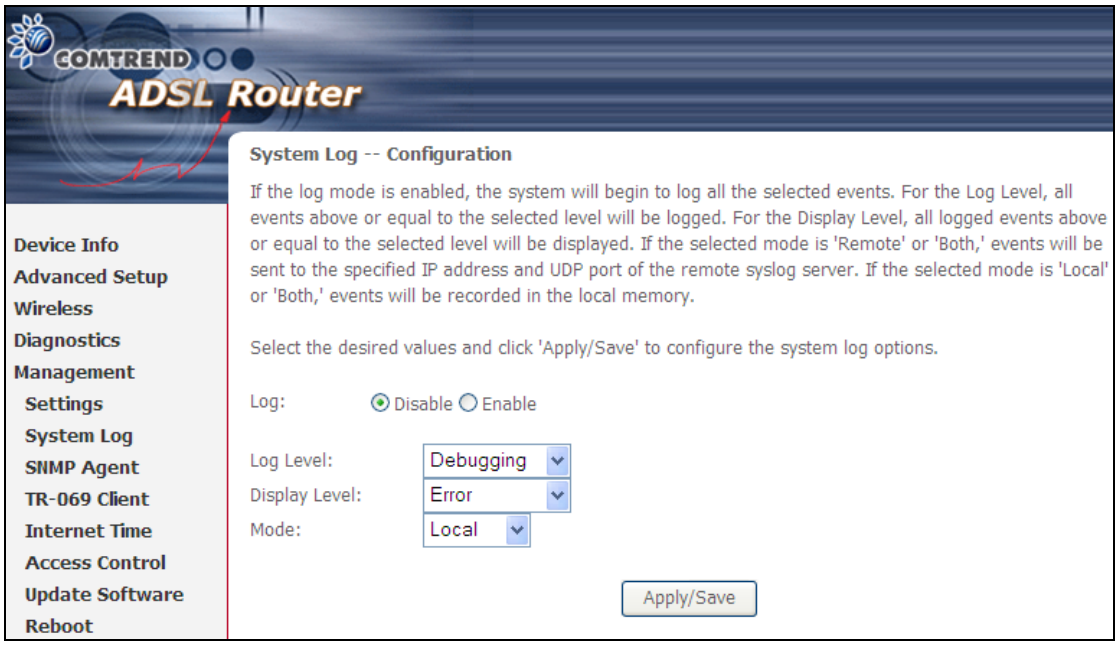
This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click **Configure System Log**, as shown below (circled in **Red**).



STEP 2: Select desired options and click **Apply/Save**.

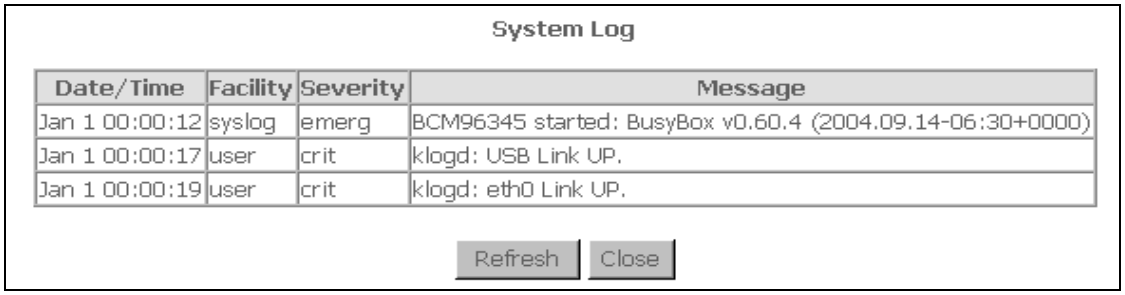

COMTREND
ADSL Router
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Apply/Save' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Apply/Save
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Reboot

Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the **Enable** radio button and then click **Apply/Save**.

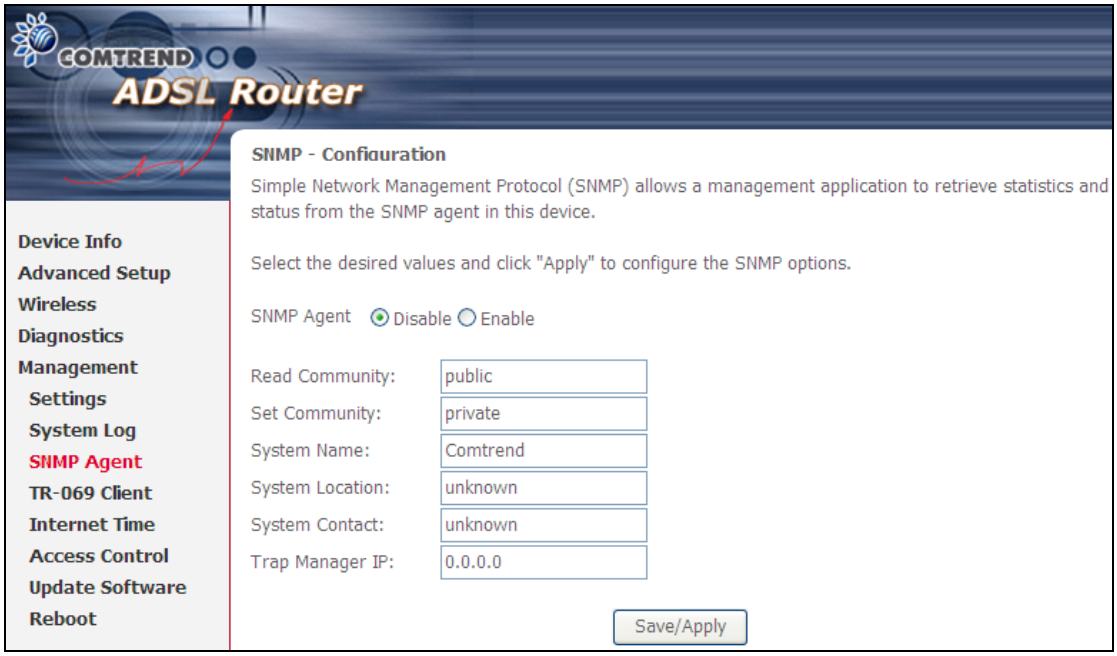
Option	Description
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the AR-5389 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

STEP 3: Click **View System Log**. The results are displayed as follows.



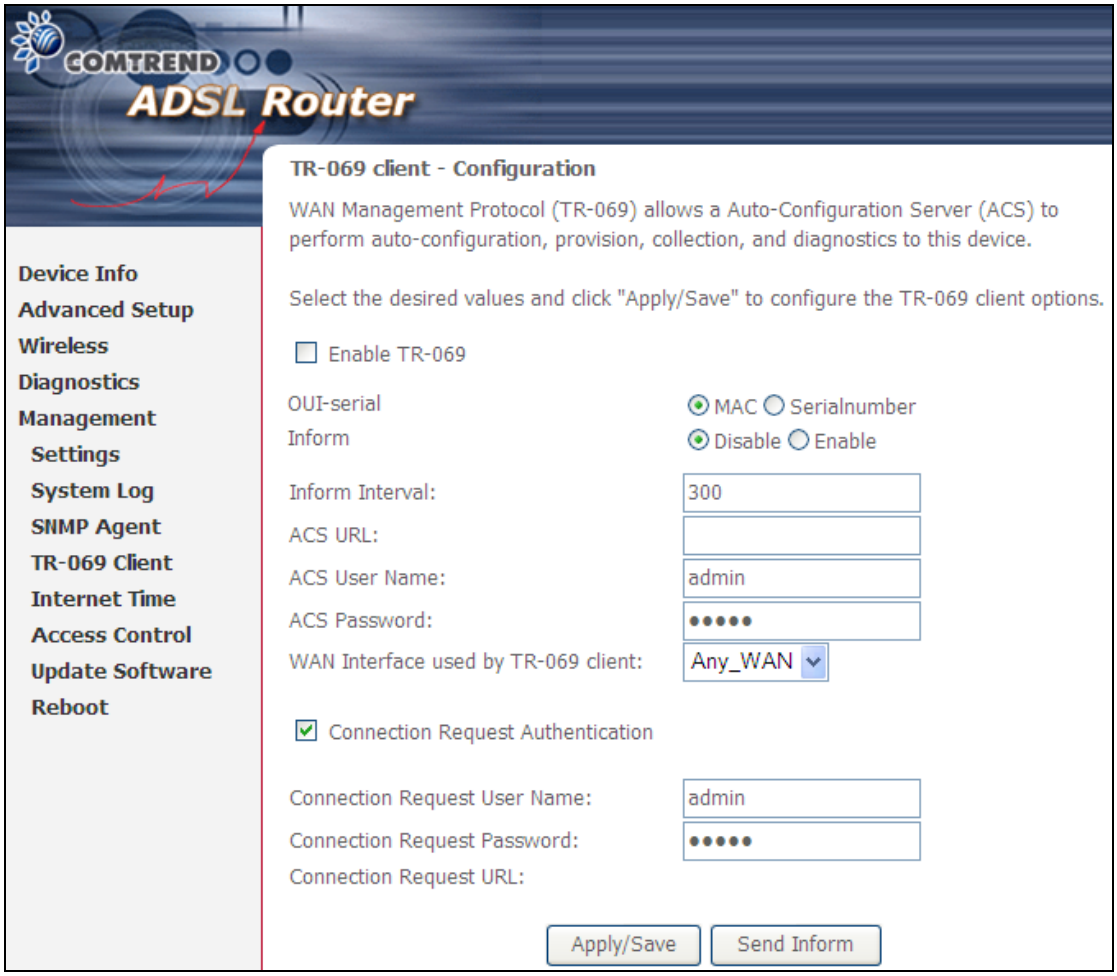
8.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save / Apply** to activate SNMP.



8.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.



The table below is provided for ease of reference.

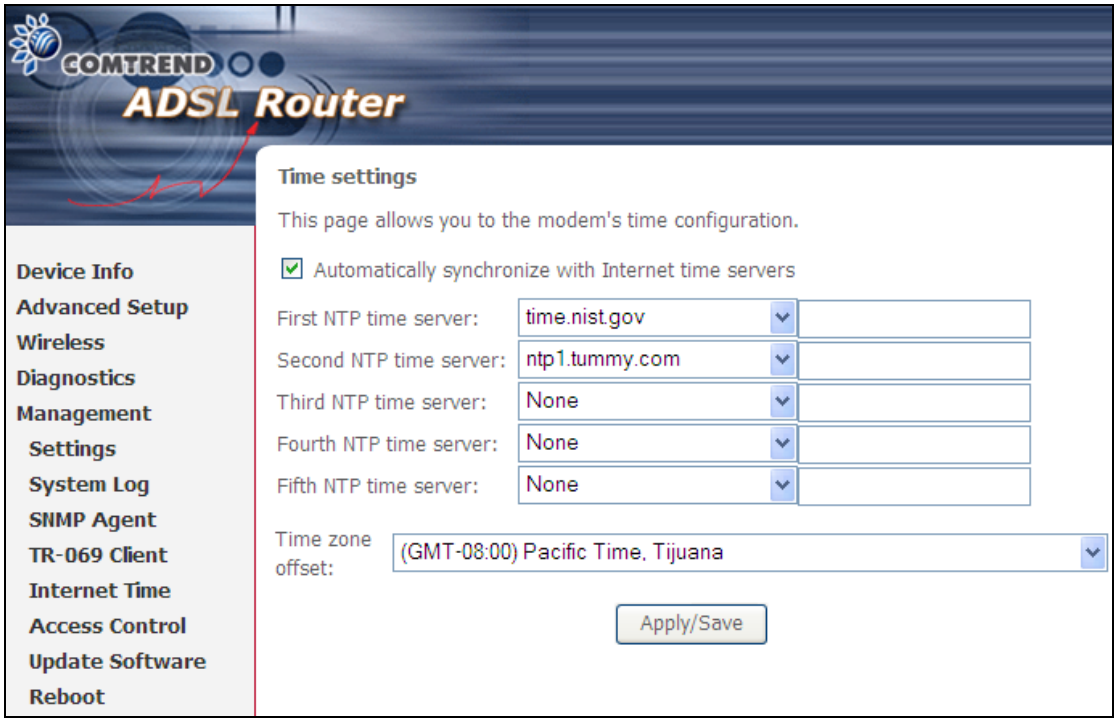
Option	Description
Enable TR-069	Tick the checkbox ☑ to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with ACS or select serial number to use router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.

Option	Description
CS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The “host” portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Connection Request	
Authorization	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to AR-5389.

The **Send Inform** button forces the CPE to establish an immediate connection to the ACS.

8.5 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox ☑, choose your preferred time server(s), select the correct time zone offset, and click **Apply / Save.**



NOTE:	In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

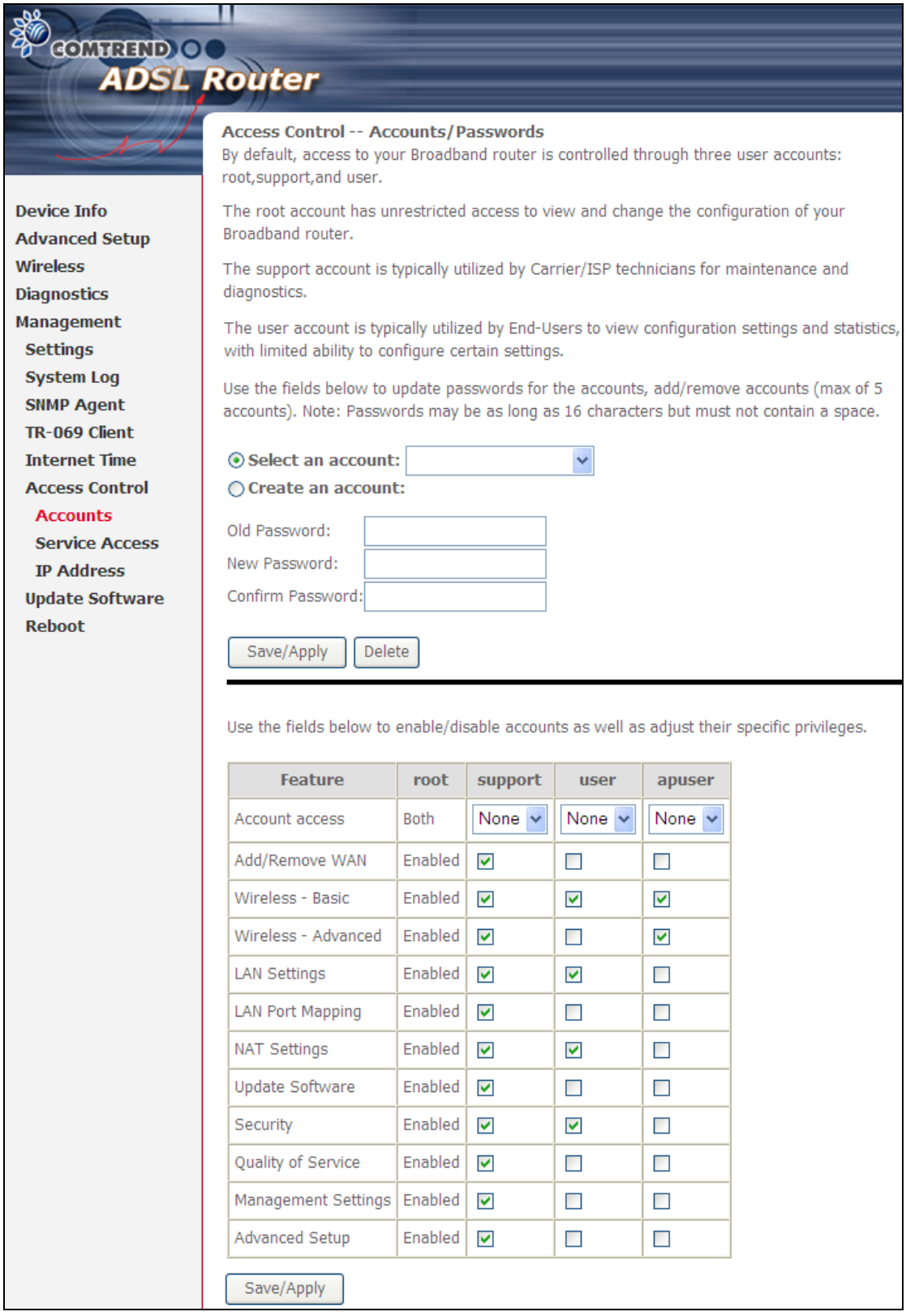
8.6 Access Control

8.6.1 Accounts/Passwords

This screen is used to configure the user account access passwords for the device. Access to the AR-5389 is controlled through the following user accounts:

- **root** - unrestricted access to change and view the configuration.
- **support** - typically utilized by Carrier/ISP technicians for maintenance and diagnostics.
- **user** - can view configuration settings & statistics and update firmware.
- **apuser** - can configure wireless settings

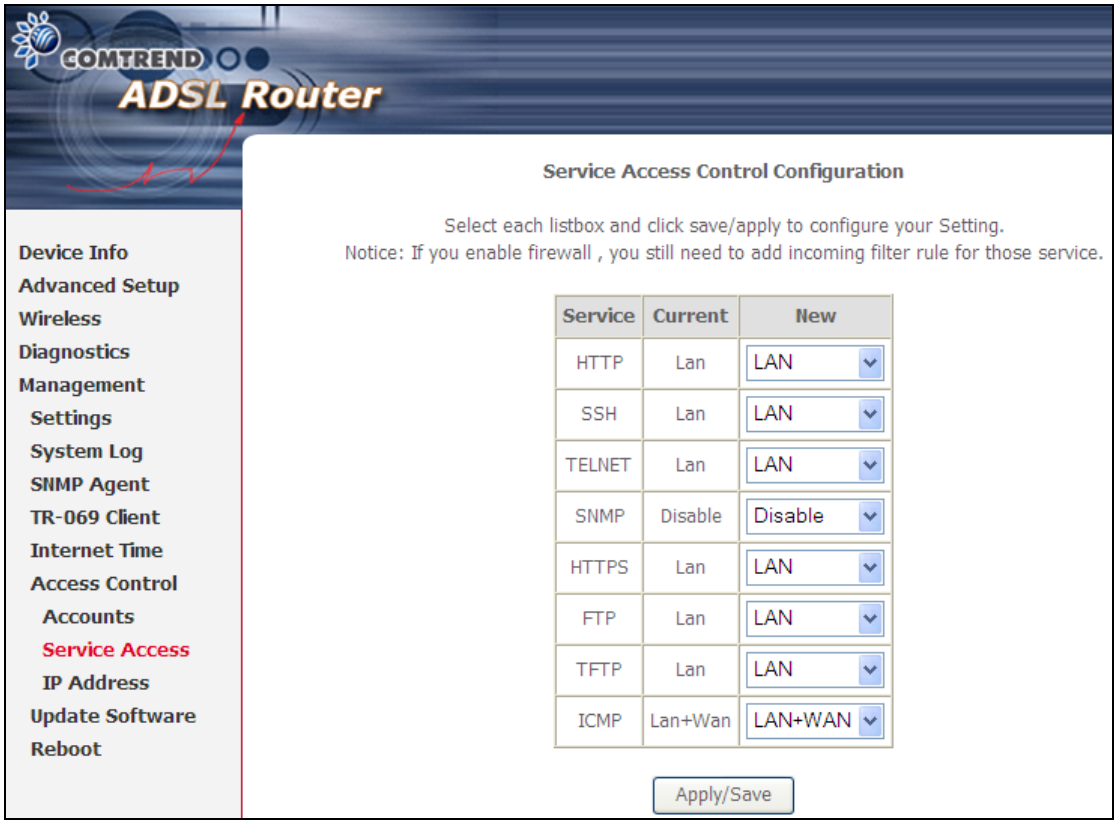
Use the fields below to change password settings and privileges. Click **Save/Apply** to continue.



NOTE: Passwords can be up to 16 characters in length.

8.6.2 Service Access

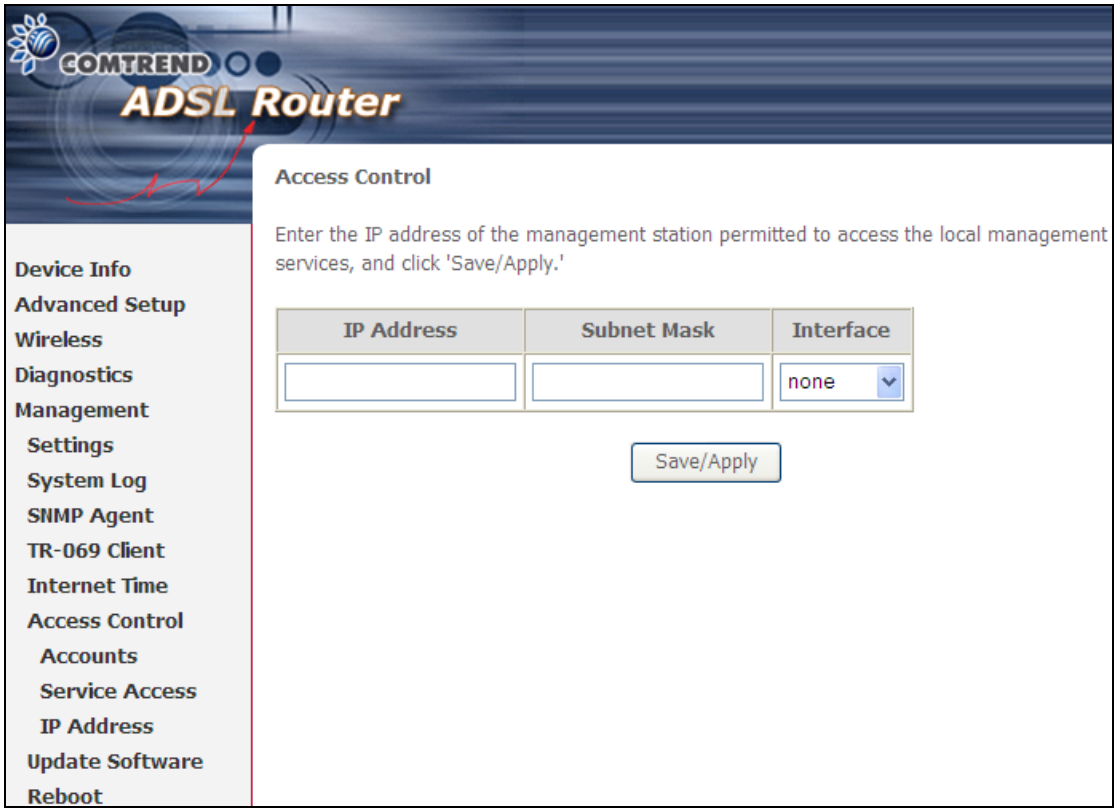
The Services option limits or opens the access services over the LAN or WAN. These access services available are: FTP, HTTP, ICMP, SNMP, TELNET and TFTP. Enable a service by selecting its dropdown listbox. Click **SAVE / APPLY** to activate.



8.6.3 IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List **beside ICMP**.

Click the Add button to display the following.



Configure the address and subnet of the management station permitted to access the local management services, and click **Save/Apply**.

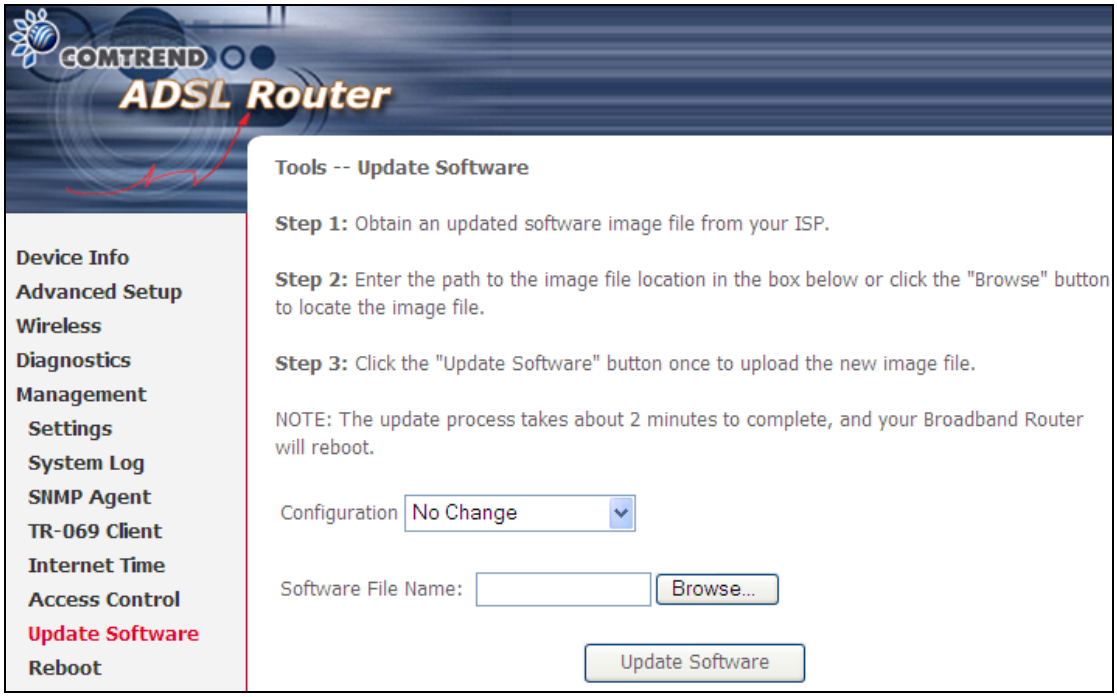
IP Address – IP address of the management station.

Subnet Mask – Subnet address for the management station.

Interface – Access permission for the specified address, allowing the address to access the local management service from none/lan/wan/lan&wan interfaces.

8.7 Update Software

This option allows for firmware upgrades from a locally stored file.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Reboot
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Configuration
No Change
Software File Name:
Browse...
Update Software

Configuration: Select for the three options available.

STEP 1: Obtain an updated software image file from your ISP.

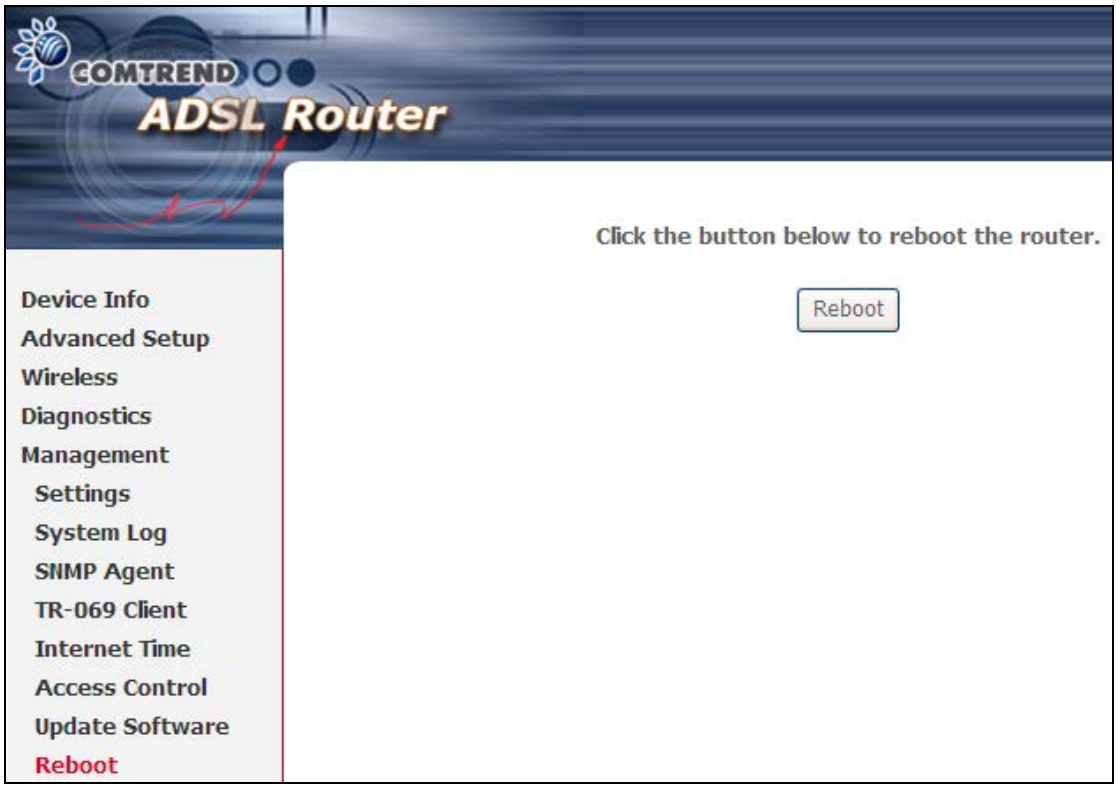
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 3: Click the **Update Software** button once to upload and install the file.

NOTE:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Chapter 4 Device Information screen with the firmware version installed, to confirm the installation was successful.

8.8 Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.



NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

Appendix A - Firewall

STATEFUL PACKET INSPECTION
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER
These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER
Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Example 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source IP address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source IP Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Dest. IP Address	: 172.16.13.4
Dest. Subnet Mask	: 255.255.255.0
Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER
Helps in setting rules to Allow or Deny packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in Bridge mode. After a Bridge mode connection is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Example 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

Appendix B – Specifications

Hardware Interface

- RJ-11 X 1 for ADSL
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- WPS Button X 1
- Wi-Fi On/Off Button X 1
- Power Switch X 1
- Wi-Fi Antenna X 1

WAN Interface

- Downstream up to 8M for ADSL, 24 Mbps for ADSL2+; Upstream up to 1Mbps,for ANNEX M Upstream up to 2.4Mbps
- ANSI T1.413 issue 2, ITU-T G.992.2 Annex A (G.lite), ITU-T G.992.3 Annex A, L, M (ADSL2), TU-T G.992.5 Annex A, M (ADSL2+), ITU-T G 994.1, ITU-T G.997.1, ETSI ETR-328

LAN Interface

- Standard IEEE 802.3, IEEE 802.3u

Wireless Interface

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
- 11 Channels (US, Canada)/ 13 Channels (Europe)/ 14 Channels (Japan)
- WPA/WPA2 Yes

Management

- SNMP V2C
- Remote upgrade
- TFTP/FTP upgrade
- Support TR069
- Telnet remote access support
- Support Web based configuration
- Support for backup & restore configuration to/from PC
- Support TR-64 for LAN management

Networking Protocols

- ARFC 2684 IP Bridging
- RFC 2684 IP Routing
- RFC 2516, PPPoE (Point over Ethernet) over ATM
- RFC 2364 PPPoA
- Support 8 PVCs
- QoS based on PVC
- Routing: RIP v1, RIP v2
- Support Static Routing
- NAT & PAT (RFC 1631)
- DMZ support
- NAT with Application Layer Gateway
- IP Routing: TCP, UDP, ICMP, ARP

- DHCP Client/Server for IP management
- DHCP Relay
- IP multicasting IGMP v1/v2
- Pass through/open/redirection and port mapping
- The Range of private IP support 192.168.1.2 to 192.168.1.254
- QoS mechanism support for mapping of PVC with different traffic classes
- HTTP (web based) for firmware upgrade & configuration
- IP filtering & raw filtering
- IGMP Snooping support
- IEEE 802.1D Transparent Bridging
- DNS Relay

Security Functions

- PAP, CHAP, TCP/IP/Port filtering rules
- Port triggering/Forwarding,
- Packet and MAC address filtering, Access control, SSH access

QoS

- Port-based QoS,
- 802.1 bit marking

Firewall/Filtering

- Stateful Inspection Firewall
- Stateless Packet Filter
- Denial of Service (DOS): ARP attacks, Ping attacks, Ping of Death, LAND,SYNC, Smurf, Unreachable, Teardrop
- TCP/IP/Port/interface filtering rules Support both incoming and outgoing filtering

NAT/NAPT

- Support Port Triggering and Port forwarding
- Symmetric port-overloading NAT, Full-Cone NAT
- Dynamic NAPT (NAPT N-to-1)
- Support DMZ host
- Virtual Server
- VPN Passthrough (PPTP, L2TP, IPSec)

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc.

Power Supply .....Input: 100 - 240 Vac
Output: 12 Vdc / 0.5 A

Environment Condition

Operating temperature .....0 ~ 50 degrees Celsius
Non-operating temperature.....-20 ~ 70 degrees Celsius
Humidity.....10 ~ 90% (non-condensing, standard operating)
Humidity.....5 ~ 95% (non-condensing, non-operating)

Dimensions .....143 mm (W) x 35 mm (H) x 120 mm (D)

Certifications..... CE, FCC

Kit Weight

(1*AR-5389, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM)

NOTE: Specifications are subject to change without notice

Appendix C - SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called “putty” that can be downloaded from here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for the LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: ssh -l admin 192.168.1.1

For WAN access, type: ssh -l support *WAN IP address*

To access the router using the Windows “putty” ssh client

For LAN access, type: putty -ssh -l admin 192.168.1.1

For WAN access, type: putty -ssh -l support *WAN IP address*

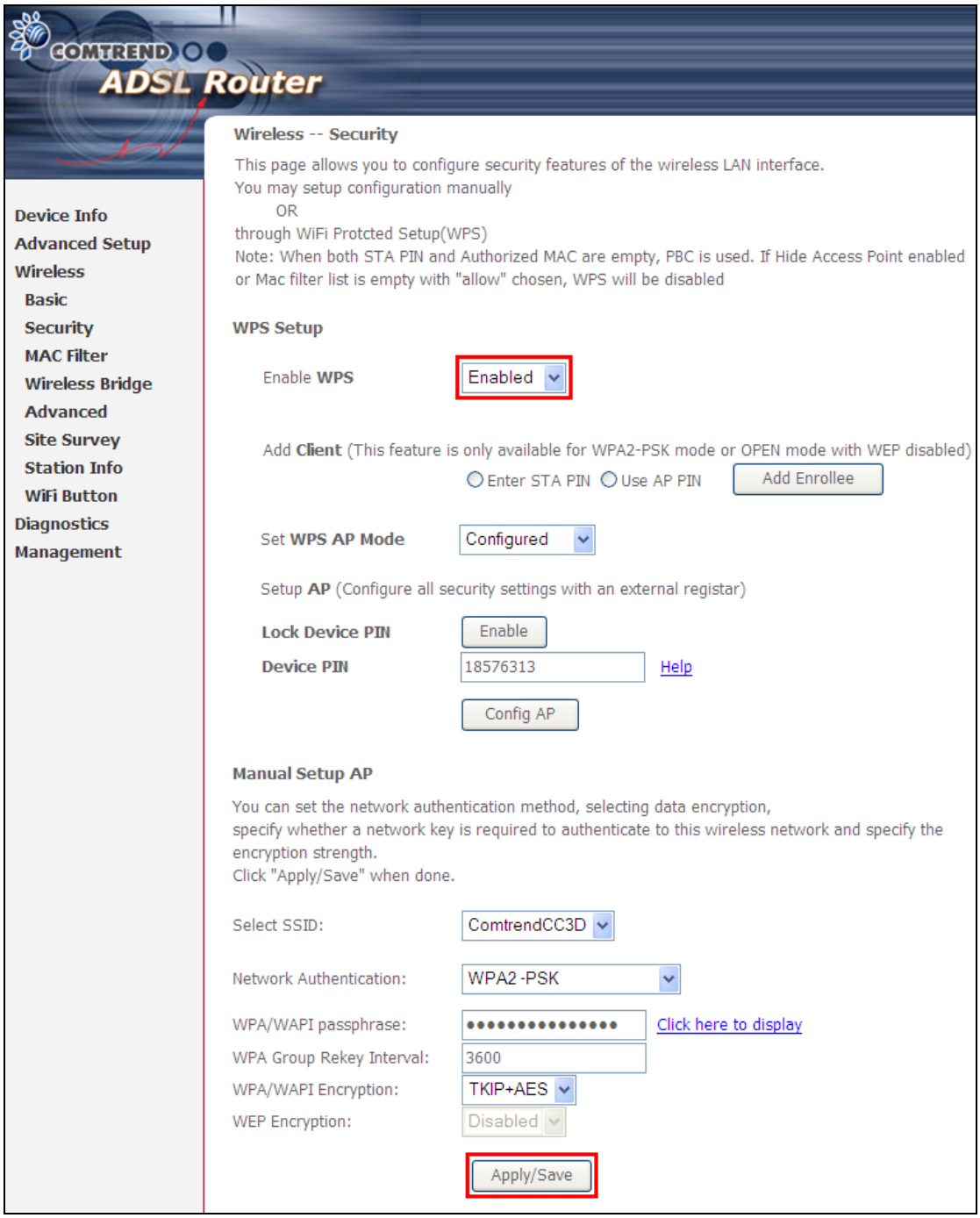
NOTE: The *WAN IP address* can be found on the Device Info → WAN screen

Appendix D - WPS OPERATION

This Section shows the basic AP WPS Operation procedure.

D1 Add Enrollee with Pin Method

1) Select **Enabled** from the Enable WPS dropdown menu.
2) Click the **Apply/Save** button at the bottom of the screen.



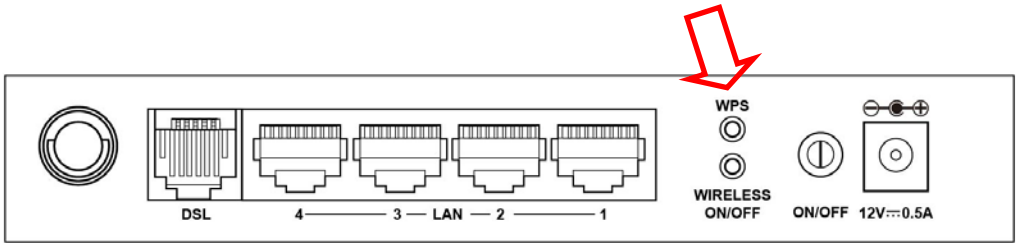
3) When the screen refreshes select the Radio button “Enter STA Pin”

4) Input Pin from Enrollee Station (67782789 in this example)
5) Click “Add Enrollee”

4) Operate Station to start WPS Adding Enrollee.

D2 Add Enrollee with PBC Method

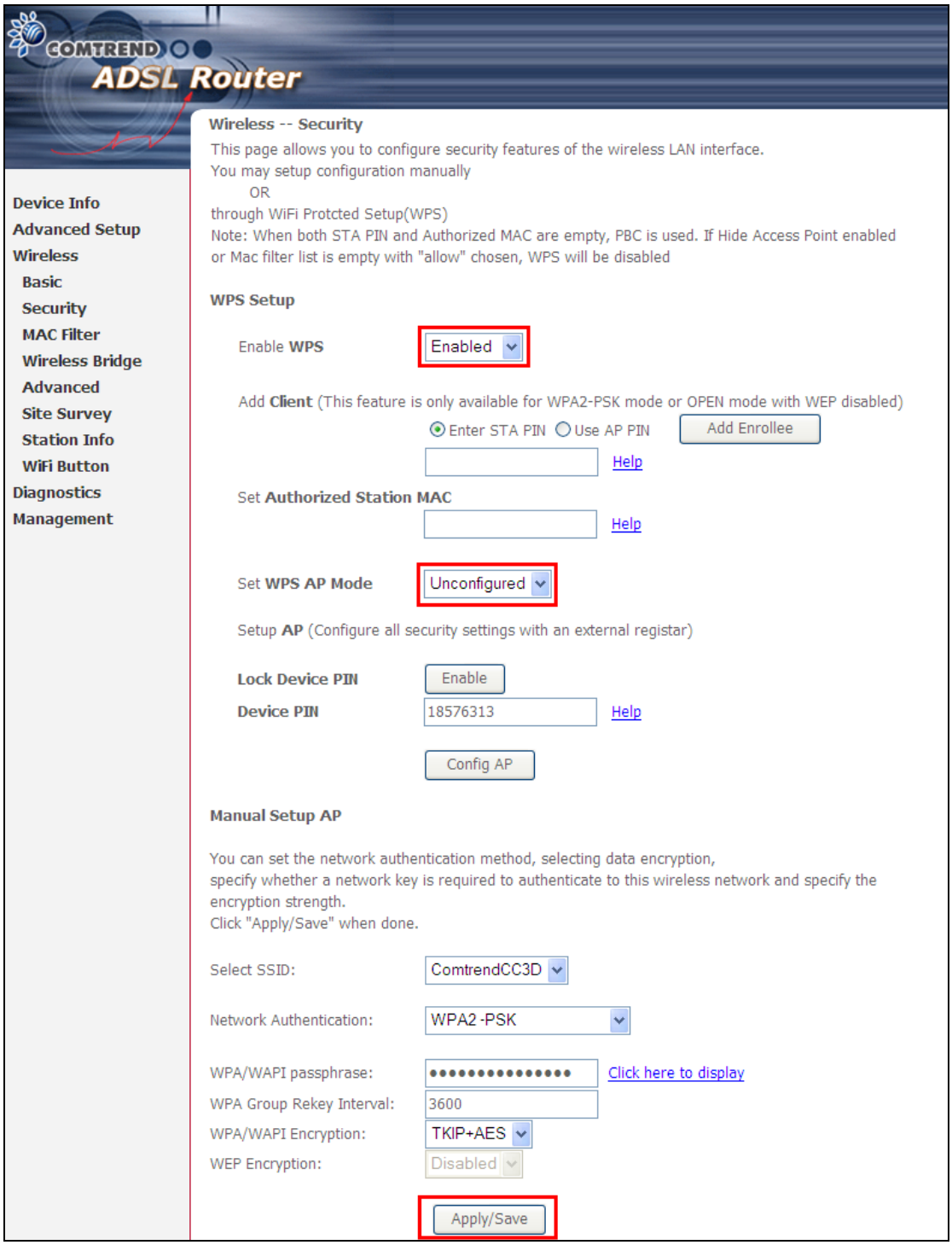
1) Press the WPS button on the rear of the device to activate WPS PBC operation.



2) Operate Station (your dongle for example) to start WPS Adding Enrollee.

D3 Configure AP

1) Select **Enabled** from the Enable WPS dropdown menu.
2) Select **Unconfigured** from the Set WPS AP Mode dropdown menu.
3) Click the **Apply/Save** button at the bottom of the screen.



The following page will show these additional items.

Lock Device PIN
When enabled, device PIN is locked and cannot be used for WPS operation.
4) Read the Device Pin (18576313 in this example) and input to External Registrar(ER – your dongle for example) when ER asks Device Pin ER could be wired (for example Windows Vista) or wireless (Intel Station).

5) Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

Appendix E - Connection Setup

Creating a WAN connection is a two-stage process.

1 - Setup a Layer 2 Interface (ATM, PTM or Ethernet).
2 - Add a WAN connection to the Layer 2 Interface.

The following sections describe each stage in turn.

E1 ~ Layer 2 Interfaces

Layer2 interface are created with a VLAN tag mode to allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not.

VLAN MUX MODE

This mode uses VLAN tags to allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not. The figure below shows multiple connections over a single VLAN Mux interface.

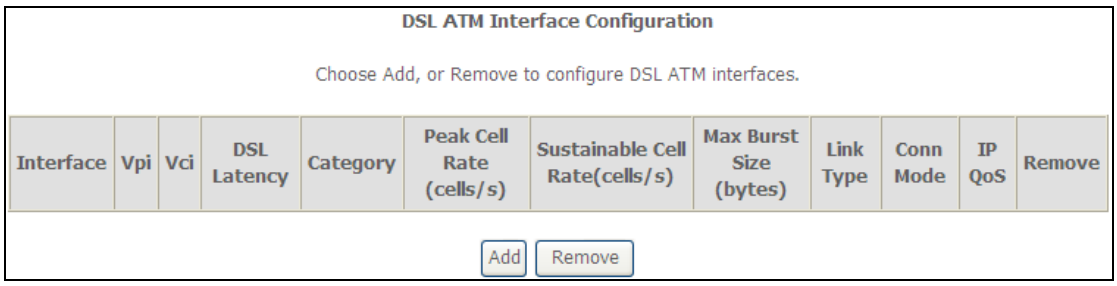
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm1.1	ipoe_0_7_77.444	IPoE	4	444	Disabled	Enabled	Disabled	Disabled	Disabled	☐	Edit
atm1.2	br_0_7_77.555	Bridge	5	555	Disabled	N/A	Disabled	Disabled	Disabled	☐	Edit
ppp1.2	pppoe_0_0_35.666	PPPoE	6	666	Disabled	Enabled	Disabled	Disabled	Disabled	☐	Edit

E1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE:	The AR-5389 supports up to 16 ATM interfaces.

STEP 1: Go to Advanced Setup → Layer2 Interface → ATM Interface.

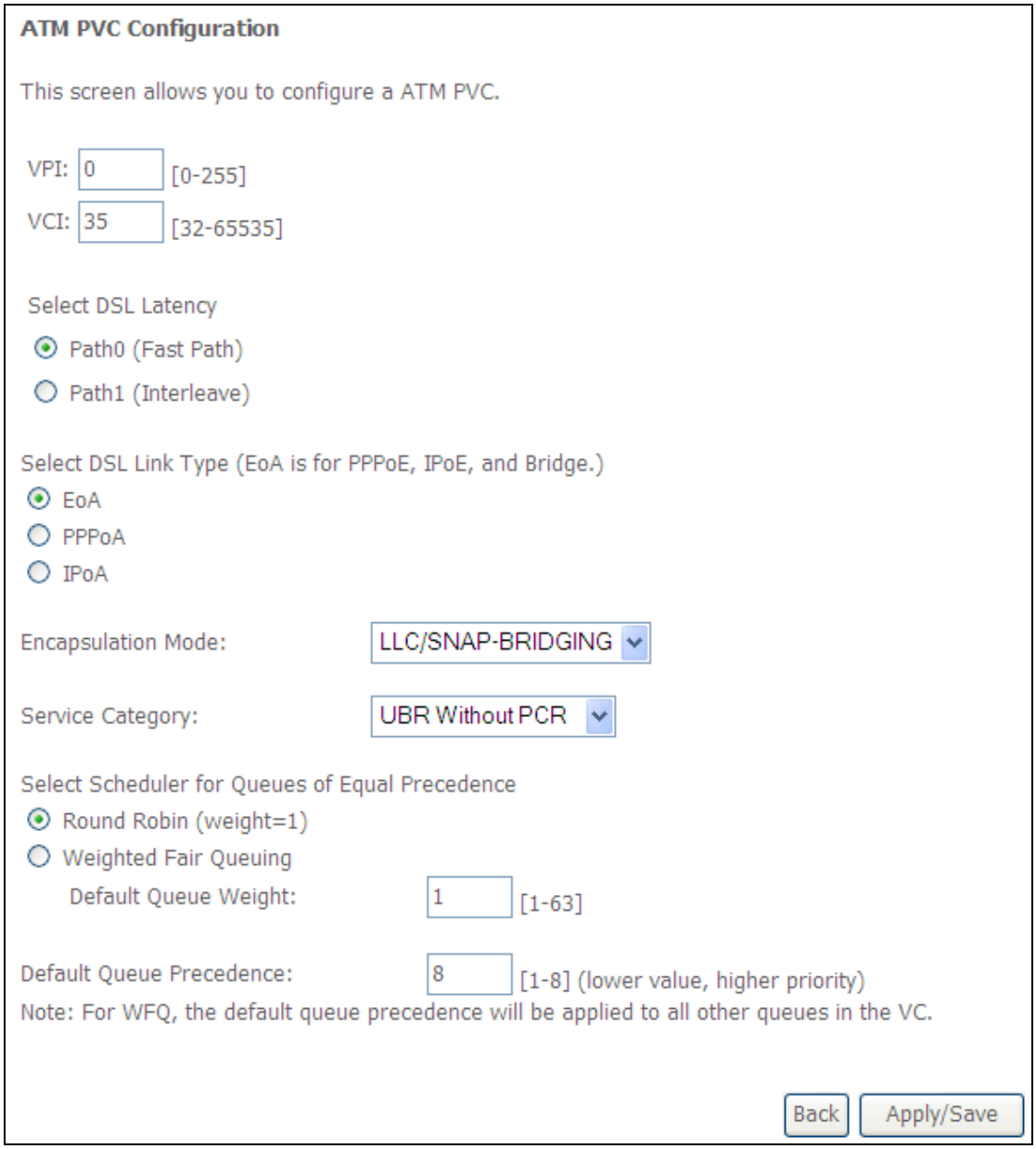


This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → port ID = 0 {Path1} → port ID = 1
Category	ATM service category
Peak Cell Rate	Maximum allowed traffic rate for the ATM PCR service connection
Sustainable Cell Rate	The average allowable, long-term cell transfer rate on the VBR service connection
Max Burst Size	The maximum allowable burst size of cells that can be transmitted contiguously on the VBR service connection
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection
IP QoS	Quality of Service (IP QoS) status
Remove	Select items for removal

STEP 2: Click **Add** to proceed to the next screen.

NOTE:	To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.


ATM PVC Configuration
This screen allows you to configure a ATM PVC.
VPI: 0 [0-255]
VCI: 35 [32-65535]
Select DSL Latency
Path0 (Fast Path)
Path1 (Interleave)
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: LLC/SNAP-BRIDGING
Service Category: UBR Without PCR
Select Scheduler for Queues of Equal Precedence
Round Robin (weight=1)
Weighted Fair Queuing
Default Queue Weight: 1 [1-63]
Default Queue Precedence: 8 [1-8] (lower value, higher priority)
Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.
Back
Apply/Save

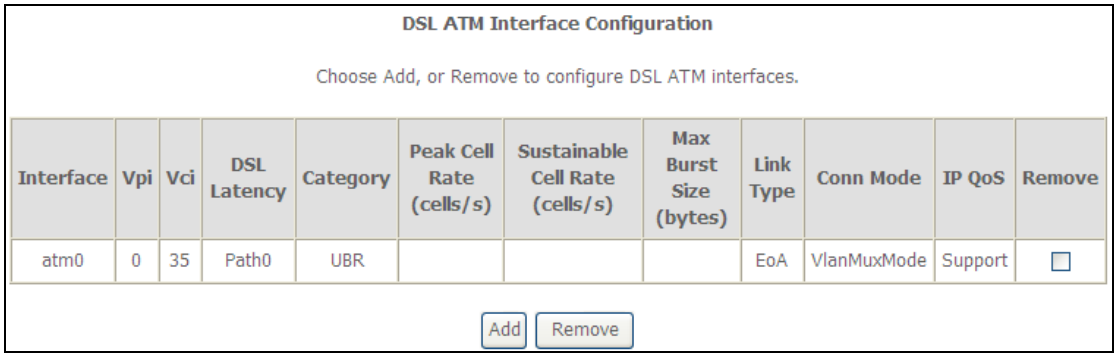
There are many settings here including: VPI/VCI, DSL Latency, DSL Link Type, Encapsulation Mode, Service Category, Connection Mode and Quality of Service.

Here are the available encapsulations for each xDSL Link Type:

- EoA- LLC/SNAP-BRIDGING, VC/MUX
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- IPoA- LLC/SNAP-ROUTING, VC MUX

STEP 3: Click **Apply/Save** to confirm your choices.

On the next screen, check that the ATM interface is added to the list. For example, an ATM interface on PVC 0/35 in Default Mode with an EoA Link type is shown below.



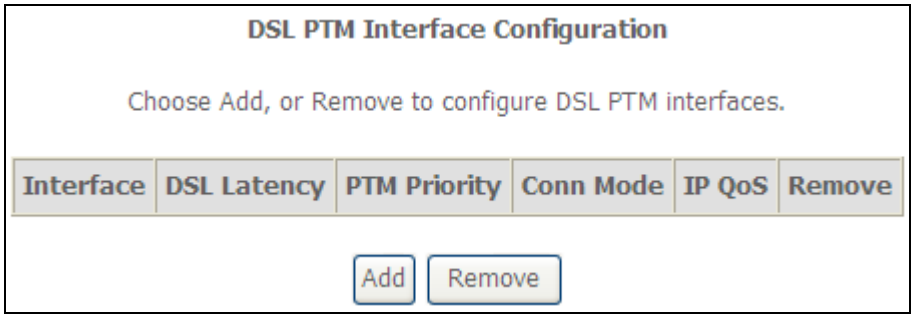
To add a WAN connection go to E2 ~ WAN Connections.

E1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

NOTE: The AR-5389 can support two PTM interfaces.

STEP 4: Go to Advanced Setup → Layer2 Interface → PTM Interface.

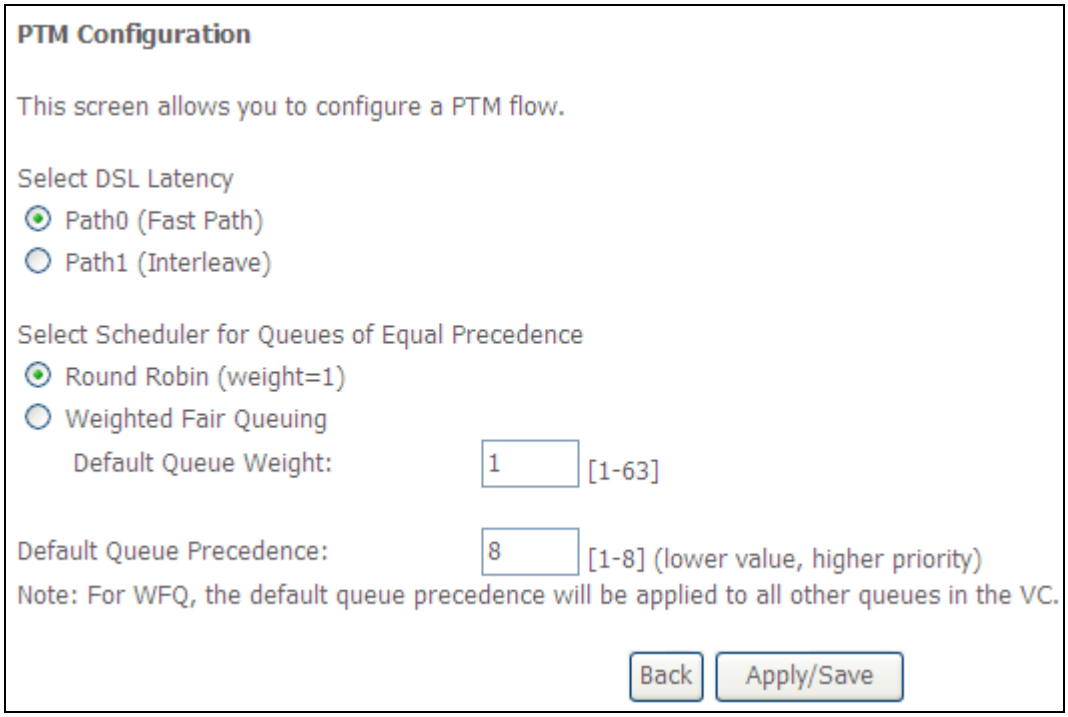


This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1
PTM Priority	Normal or High Priority (Preemption).
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. MSC Mode – Multiple Services over one interface.
QoS	Quality of Service (QoS) status.
Remove	Select interfaces to remove.

STEP 5: Click **Add** to proceed to the next screen.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

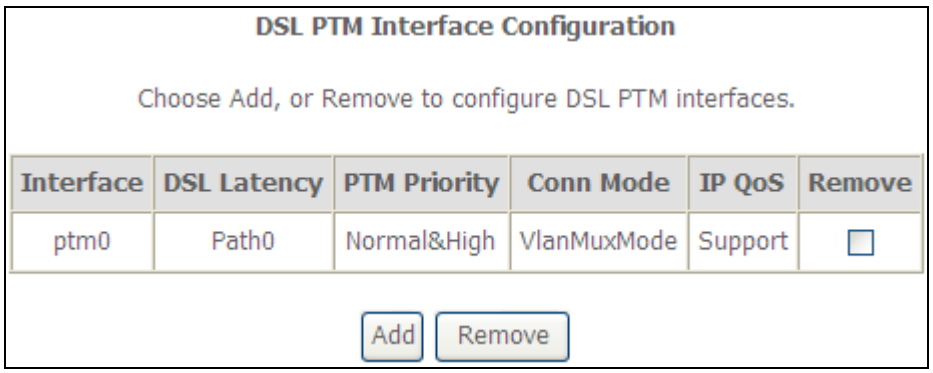


There are many settings that can be configured here including:
DSL Latency, PTM Priority, Connection Mode and Quality of Service.

STEP 6: Click **Apply/Save** to confirm your choices.

On the next screen, check that the PTM interface is added to the list.

For example, an PTM interface in Default Mode is shown below.



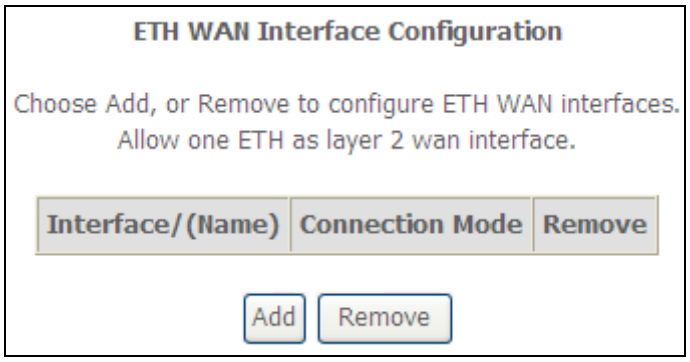
To add a WAN connection go to E2 ~ WAN Connections.

E1.3 Ethernet WAN Interface

Some models of the AR-5389 support a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet WAN interface.

NOTE:	To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

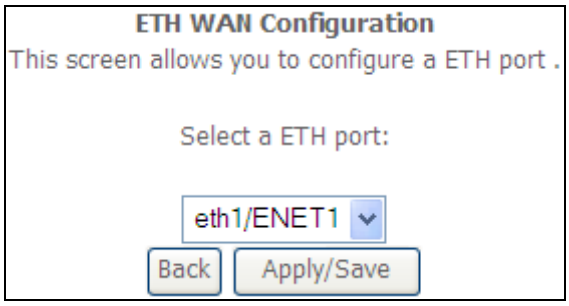
STEP 1: Go to Advanced Setup → Layer2 Interface → ETH Interface.



This table is provided here for ease of reference.

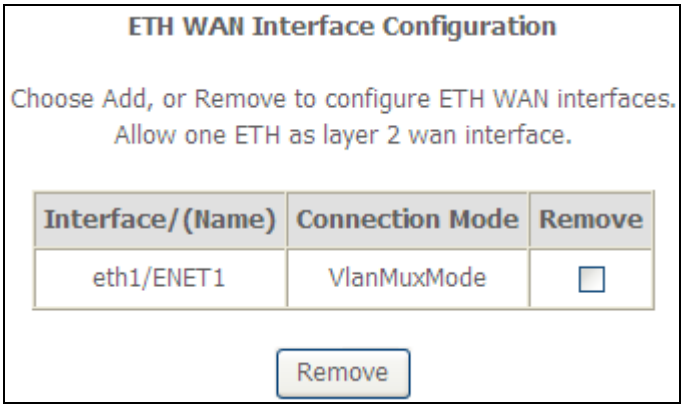
Heading	Description
Interface/ (Name)	ETH WAN Interface
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection MSC Mode – Multiple Service over one Connection
Remove	Select the checkbox and click **Remove** to remove the connection.

STEP 2: Click **Add** to proceed to the next screen.



STEP 3: **STEP 4:** Click **Apply/Save** to confirm your choice.

The figure below shows an Ethernet WAN interface configured in VlanMuxMode.



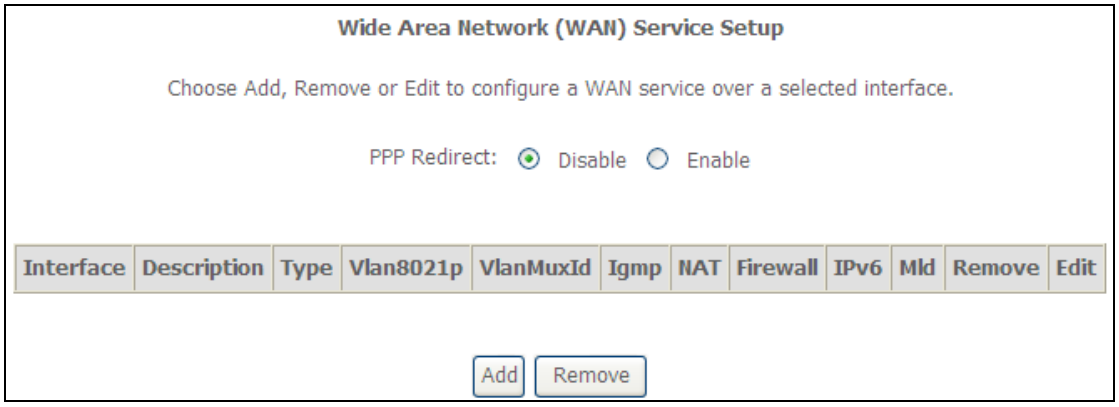
To add a WAN connection go to Appendix E - Connection Setup.

E2 ~ WAN Connections

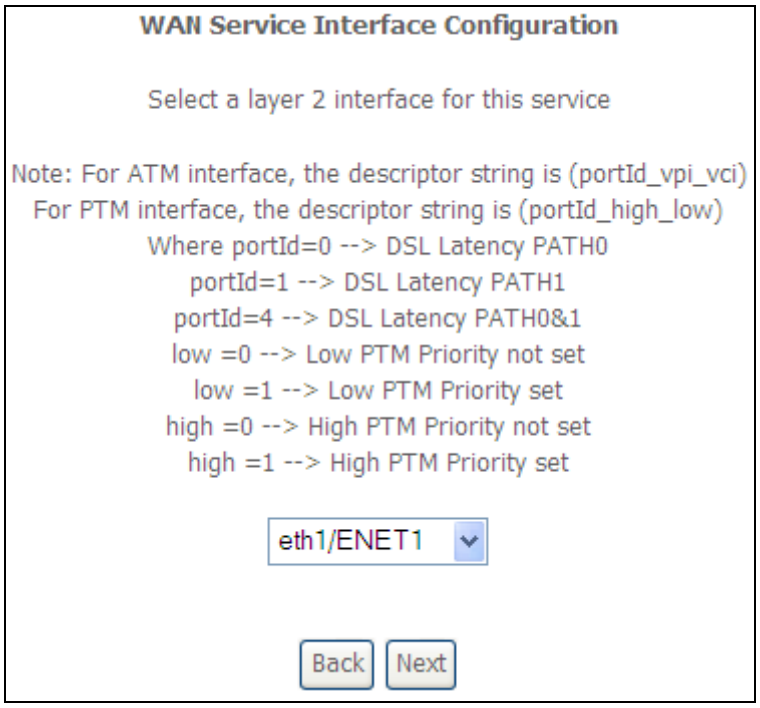
In Default Mode, the AR-5389 supports up to 16 connections.

To setup a WAN connection follow these instructions.

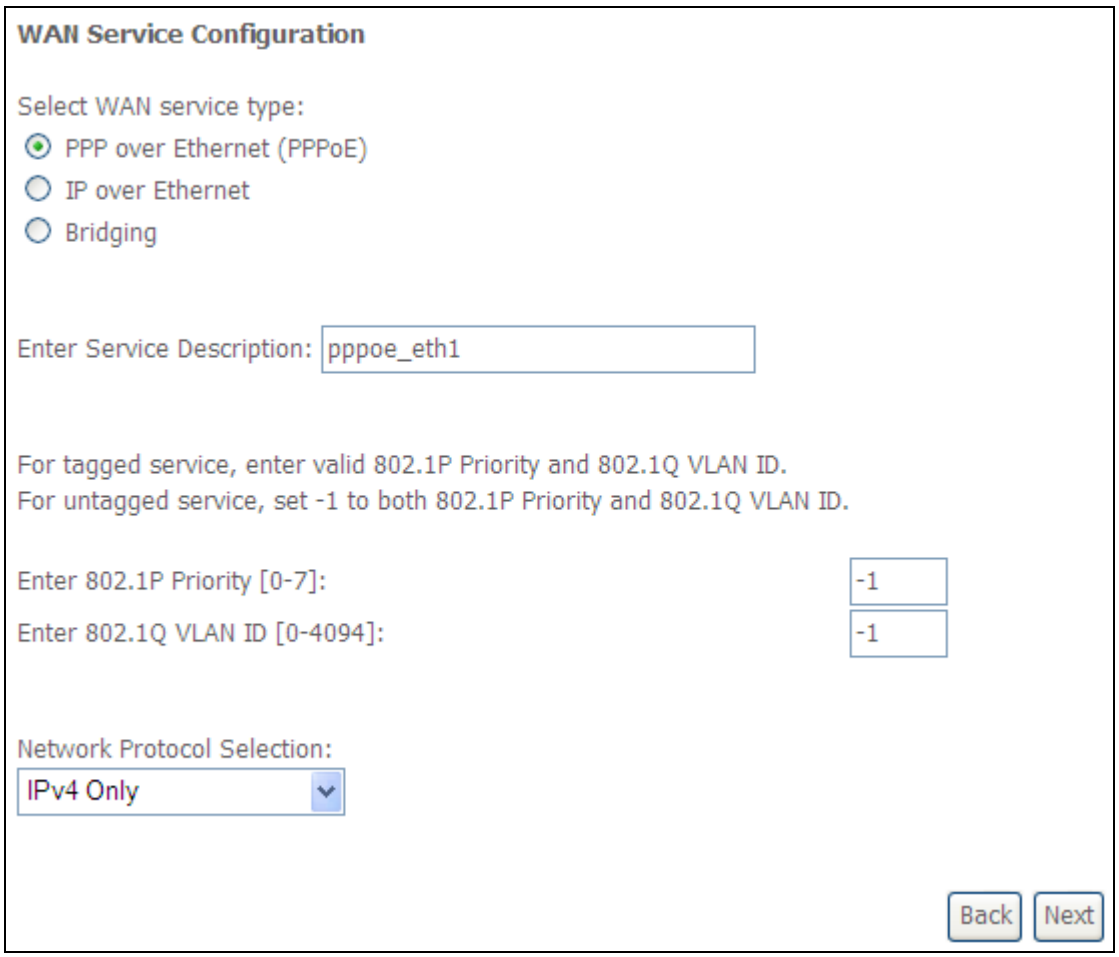
STEP 1: Go to the Advanced Setup → WAN Service screen.


Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.
PPP Redirect: Disable Enable
Interface Description Type Vlan8021p VlanMuxId Igmp NAT Firewall IPv6 Mld Remove Edit
Add Remove

STEP 2: Click **Add** to create a WAN connection. The following screen will display.

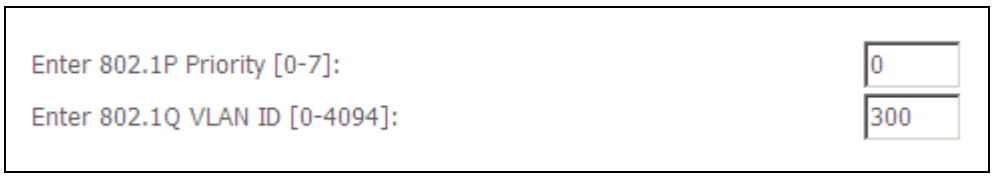

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
eth1/ENET1
Back Next

STEP 3: Choose a layer 2 interface from the drop-down box and click **Next**. The WAN Service Configuration screen will display as shown below.


WAN Service Configuration
Select WAN service type:
PPP over Ethernet (PPPoE)
IP over Ethernet
Bridging
Enter Service Description: pppoe_eth1
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.
Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1
Network Protocol Selection:
IPv4 Only
Back
Next

NOTE:	The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.

STEP 4: For VLAN Mux Connections, you must enter Priority & VLAN ID tags.



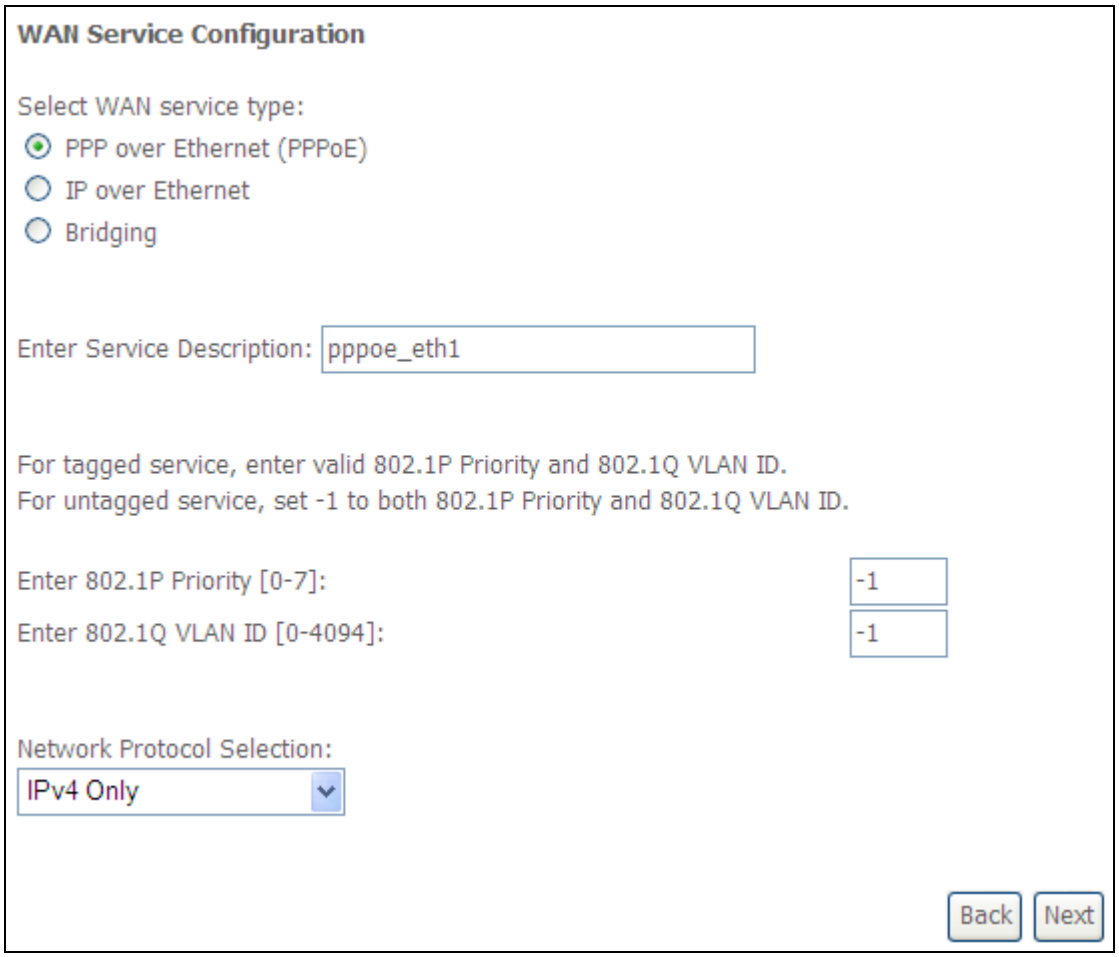
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For PPP over ETHERNET (PPPoE), go to page 155.
(2) For IP over ETHERNET (IPoE), go to page 161.
(3) For Bridging, go to page 167.
(4) For PPP over ATM (PPPoA), go to page 169.
(5) For IP over ATM (IPoA), go to page 174.

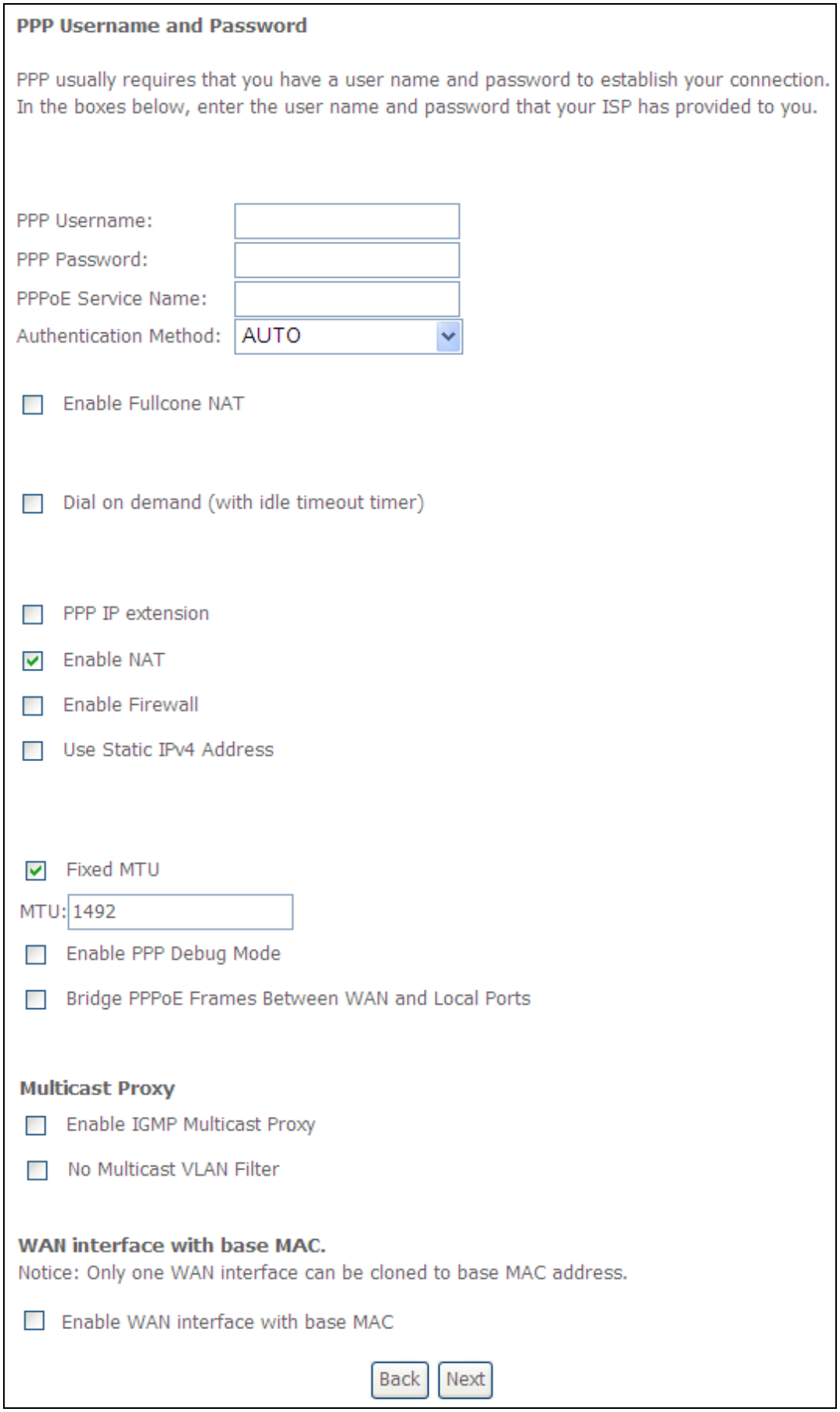
The subsections that follow continue the WAN service setup procedure.

E2.1 PPP over ETHERNET (PPPoE)

STEP 1: Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.


WAN Service Configuration
Select WAN service type:
PPP over Ethernet (PPPoE)
IP over Ethernet
Bridging
Enter Service Description: pppoe_eth1
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.
Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1
Network Protocol Selection:
IPv4 Only
Back
Next

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.

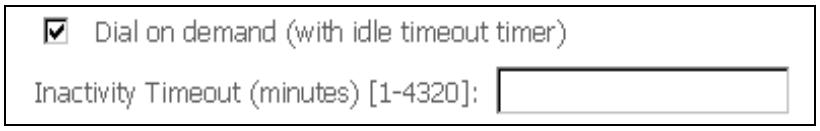

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:
AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
PPP IP extension
Enable NAT
Enable Firewall
Use Static IPv4 Address
Fixed MTU
MTU:
1492
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy
Enable IGMP Multicast Proxy
No Multicast VLAN Filter
WAN interface with base MAC.
Notice: Only one WAN interface can be cloned to base MAC address.
Enable WAN interface with base MAC
Back
Next

The settings shown above are described below.

PPP SETTINGS
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The AR-5389 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv4 Address** field.
Don't forget to adjust the IP configuration to Static IP Mode as described in Section 3.2

MTU
Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

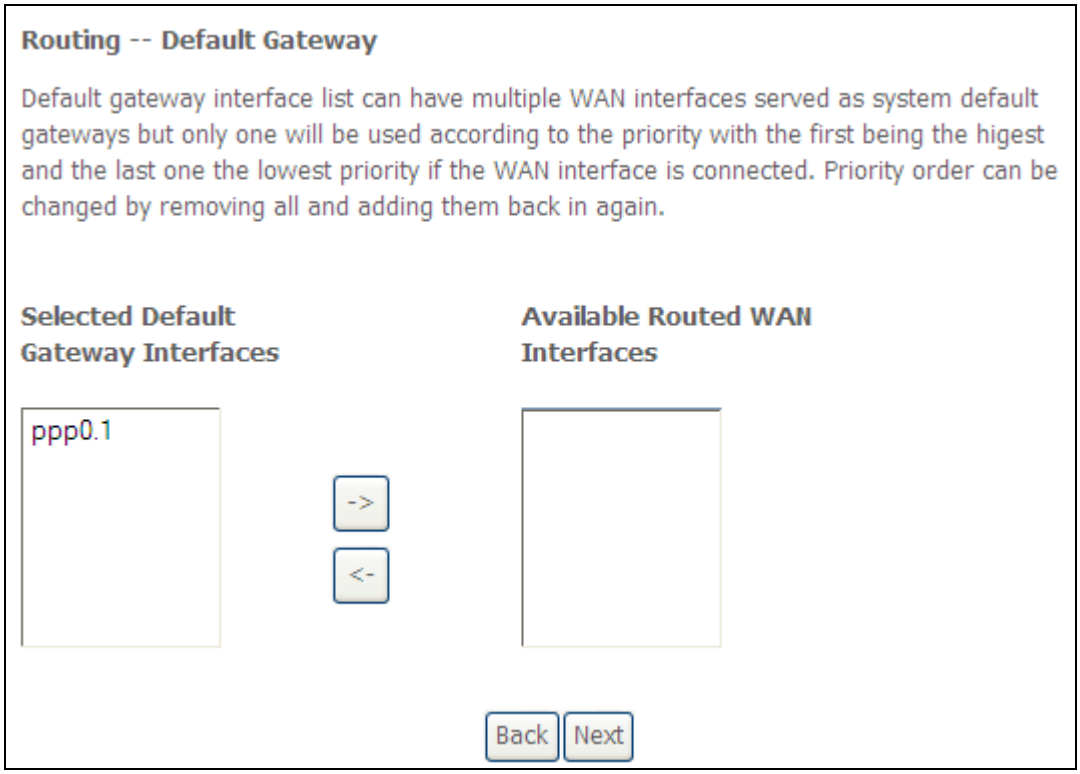
BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The AR-5389 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

NO MULTICAST VLAN FILTER
Tick the checkbox ☑ to Enable/Disable multicast VLAN filter.

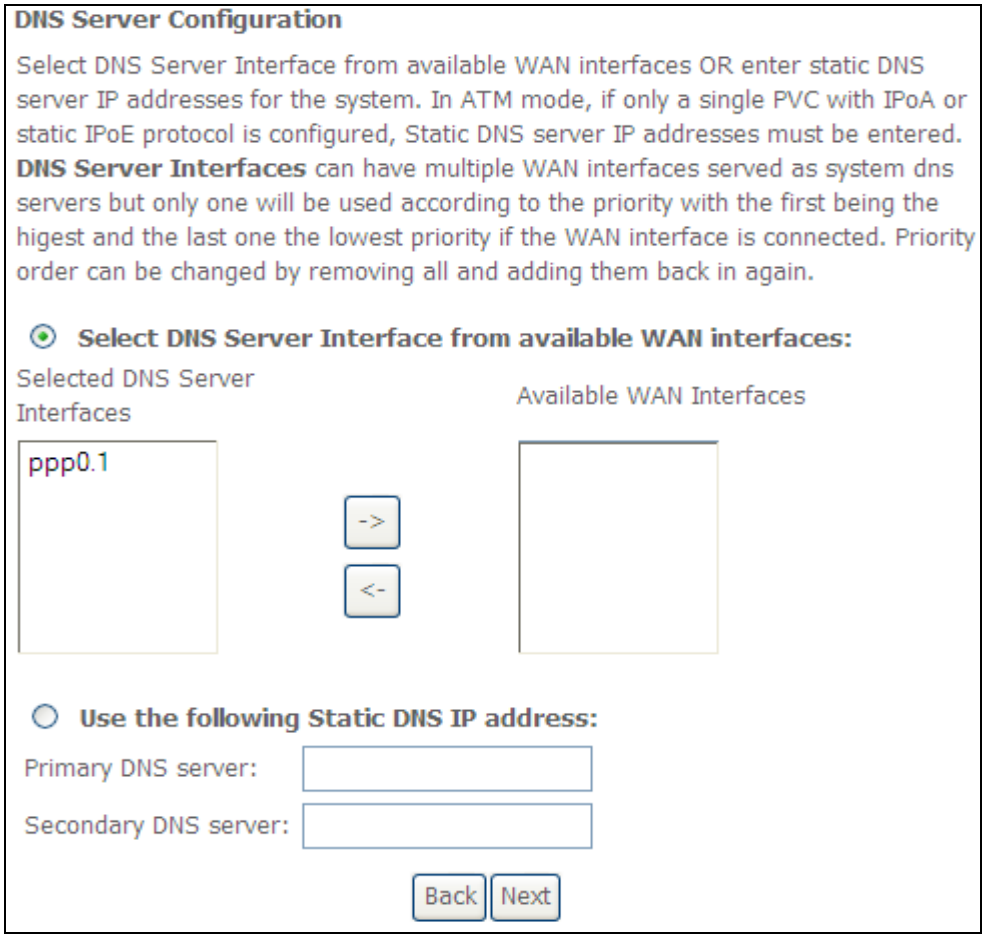
Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 3: Choose an interface to be the default gateway.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0.1
->
<-
Back
Next

Click **Next** to continue or click **Back** to return to the previous step.

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.


DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
ppp0.1
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

Click **Next** to continue or click **Back** to return to the previous step.

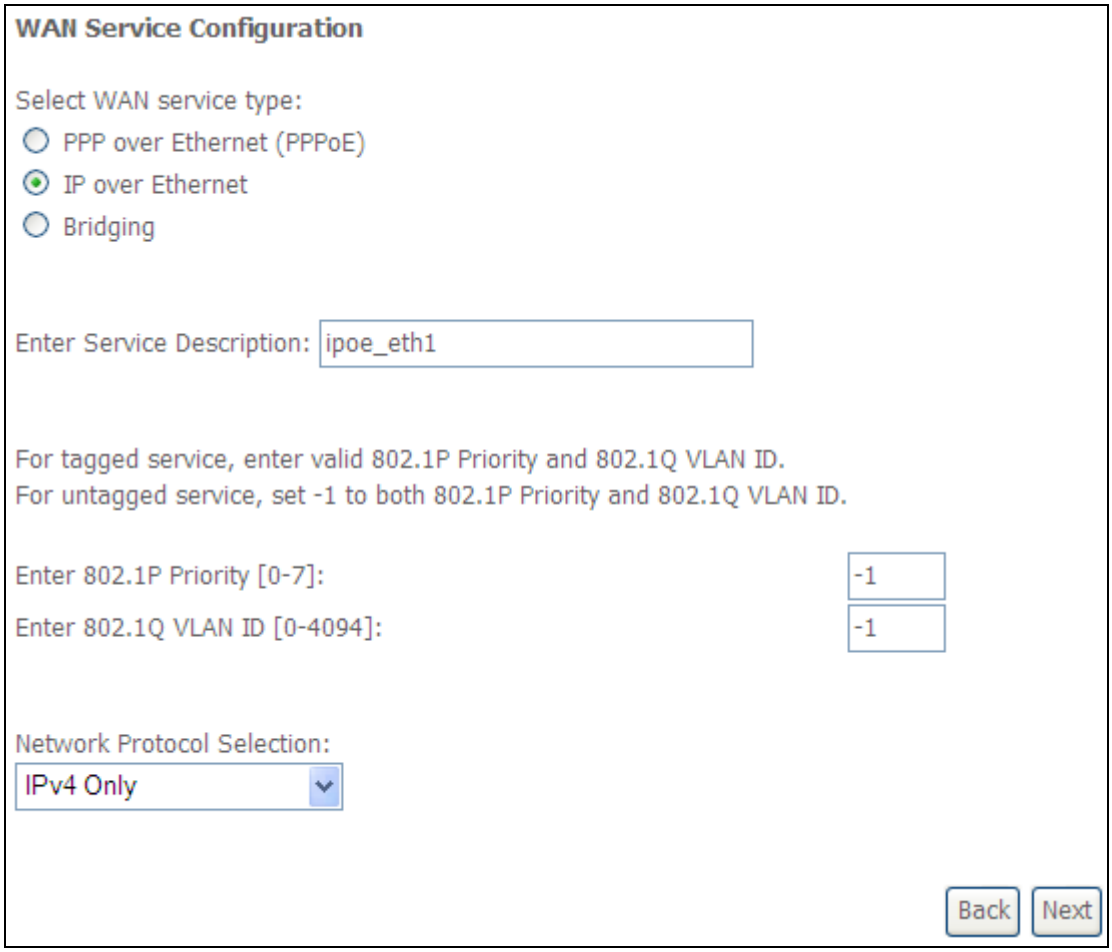
STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoE
NAT: Enabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

E2.2 IP over ETHERNET (IPoE)

STEP 1: ***Select the IP over Ethernet radio button and click **Next.**

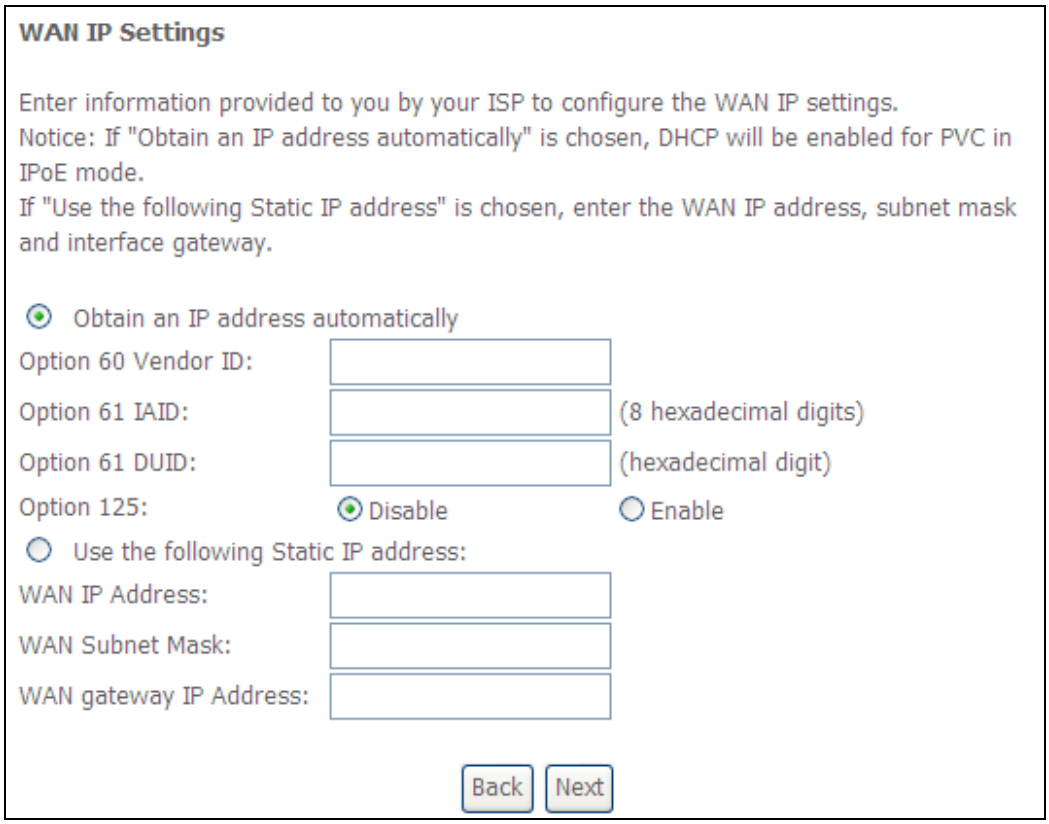

WAN Service Configuration
Select WAN service type:
PPP over Ethernet (PPPoE)
IP over Ethernet
Bridging
Enter Service Description: ipoe_eth1
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.
Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1
Network Protocol Selection:
IPv4 Only
Back
Next

*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

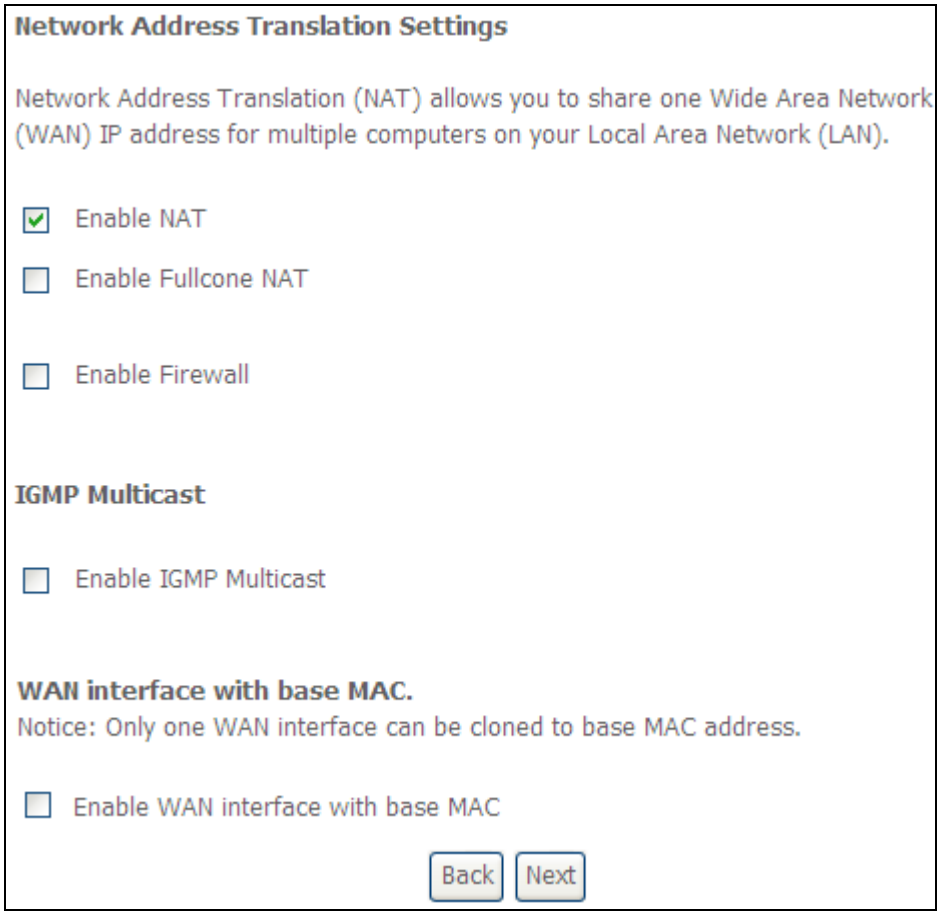
STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the **Static IP address** method to assign WAN IP address, Subnet Mask and Default Gateway manually.


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Obtain an IP address automatically
Option 60 Vendor ID:
Option 61 IAID:
(8 hexadecimal digits)
Option 61 DUID:
(hexadecimal digit)
Option 125:
Disable
Enable
Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:
Back
Next

NOTE: If IPv6 networking is enabled, an additional set of instructions, radio buttons, and text entry boxes will appear at the bottom of the screen. These configuration options are quite similar to those for IPv4 networks.

Click **Next** to continue or click **Back** to return to the previous step.

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Fullcone NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast
WAN interface with base MAC.
Notice: Only one WAN interface can be cloned to base MAC address.
Enable WAN interface with base MAC
Back
Next

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

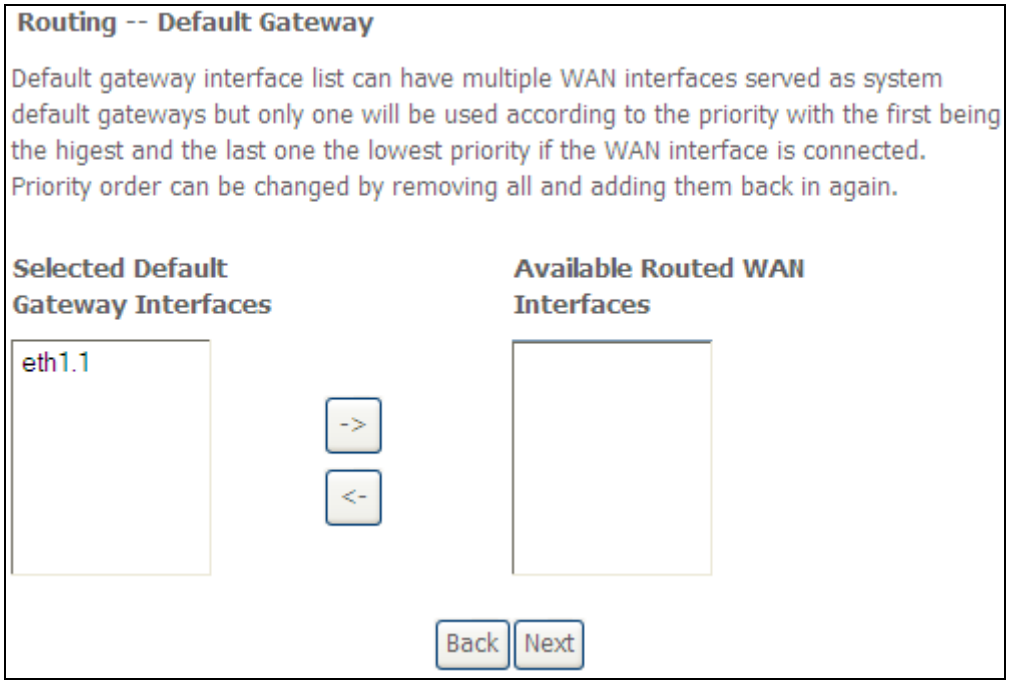
ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

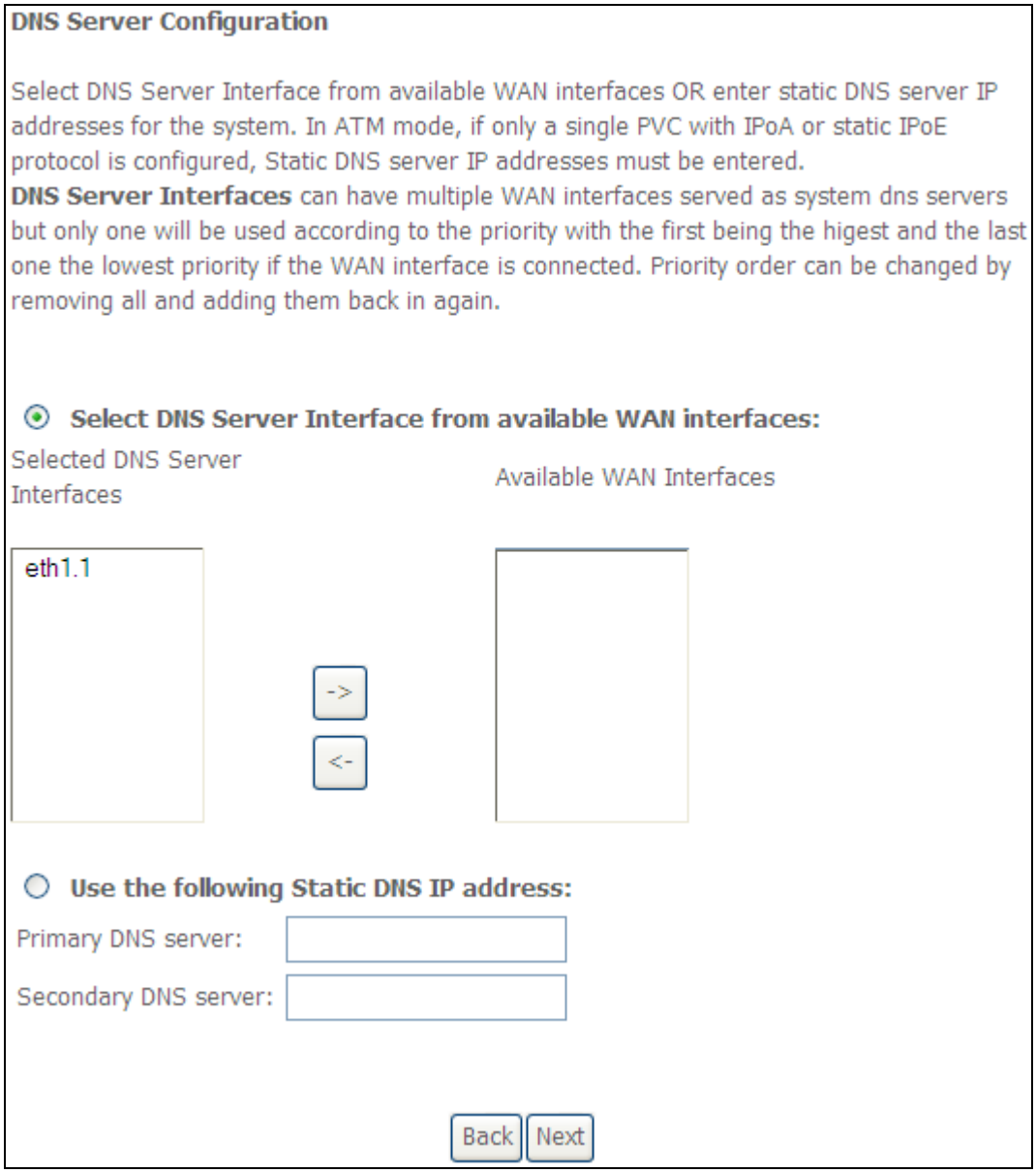
Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 4: To choose an interface to be the default gateway.

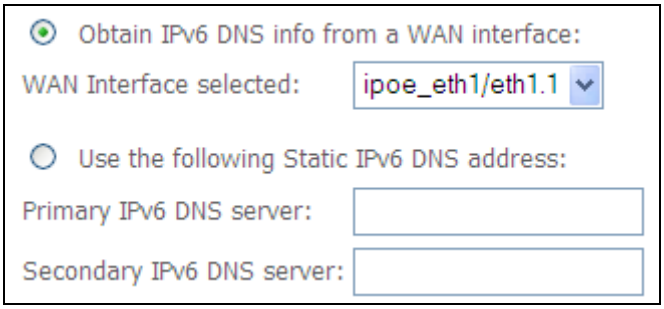

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
eth1.1
->
<-
Back
Next

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.


DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
eth1.1
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

If IPv6 is enabled, an additional set of options will be shown.

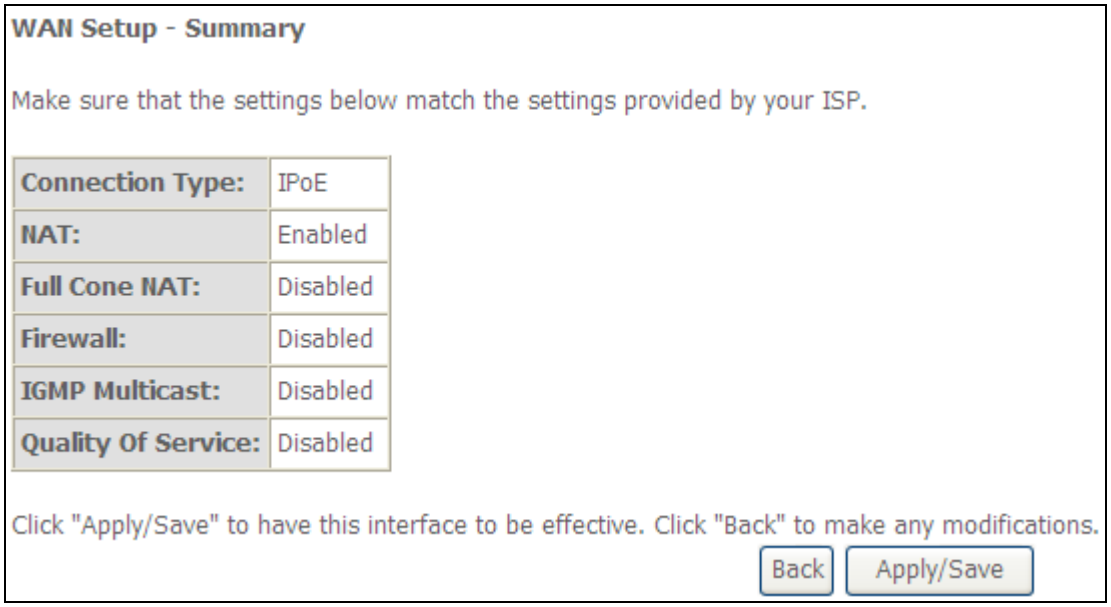

Obtain IPv6 DNS info from a WAN interface:
WAN Interface selected:
ipoe_eth1/eth1.1
Use the following Static IPv6 DNS address:
Primary IPv6 DNS server:
Secondary IPv6 DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.

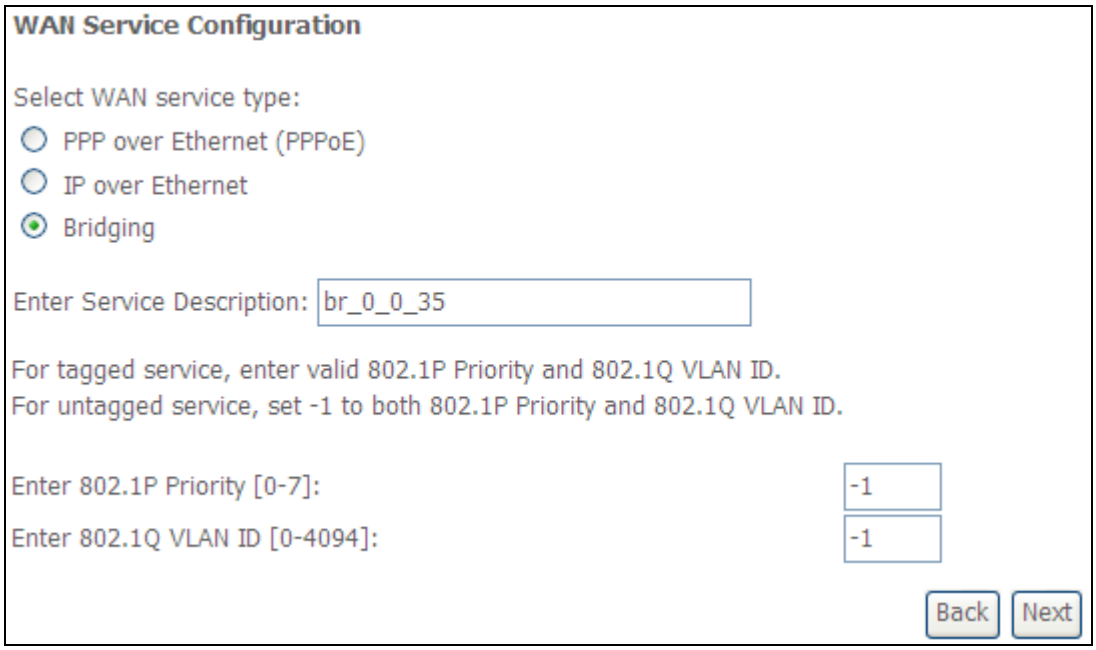

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoE
NAT: Enabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

After clicking **Apply / Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

E2.3 Bridging

NOTE:	This connection type is not available on the Ethernet WAN interface.

STEP 1: ***Select the Bridging radio button and click **Next**.

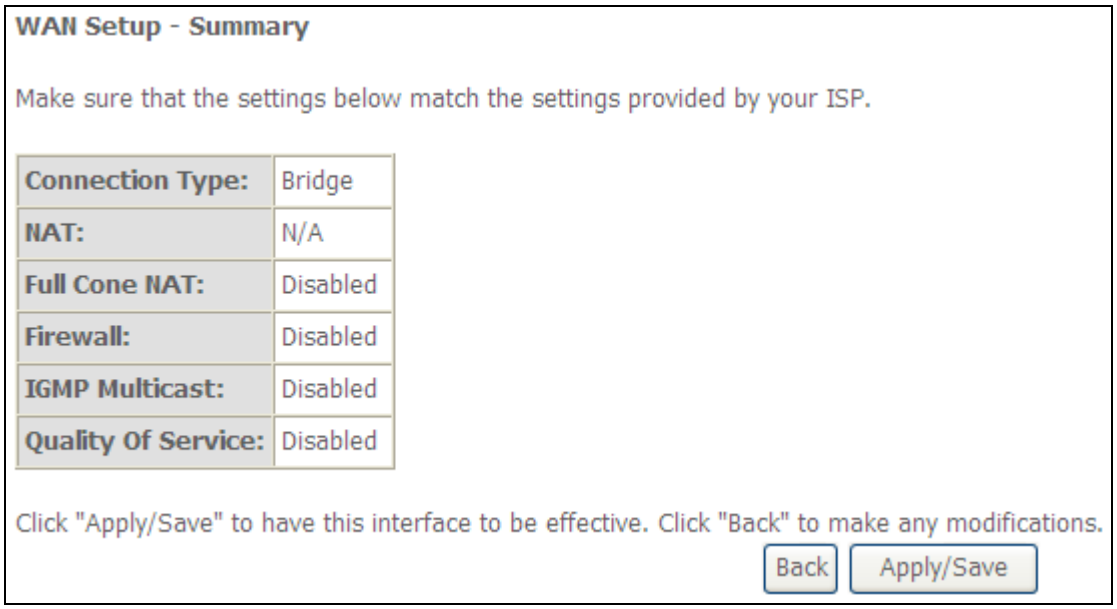

WAN Service Configuration
Select WAN service type:
PPP over Ethernet (PPPoE)
IP over Ethernet
Bridging
Enter Service Description: br_0_0_35
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.
Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1
Back
Next

*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

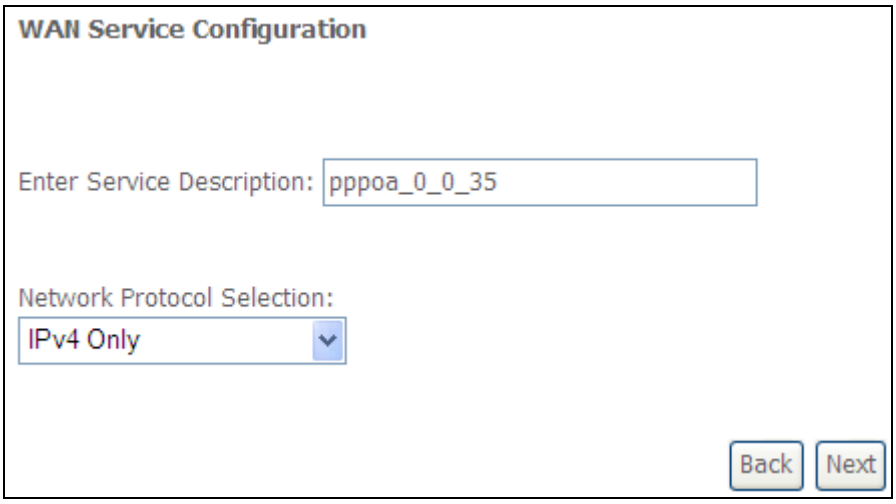
STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to return to the previous screen.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: Bridge
NAT: N/A
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

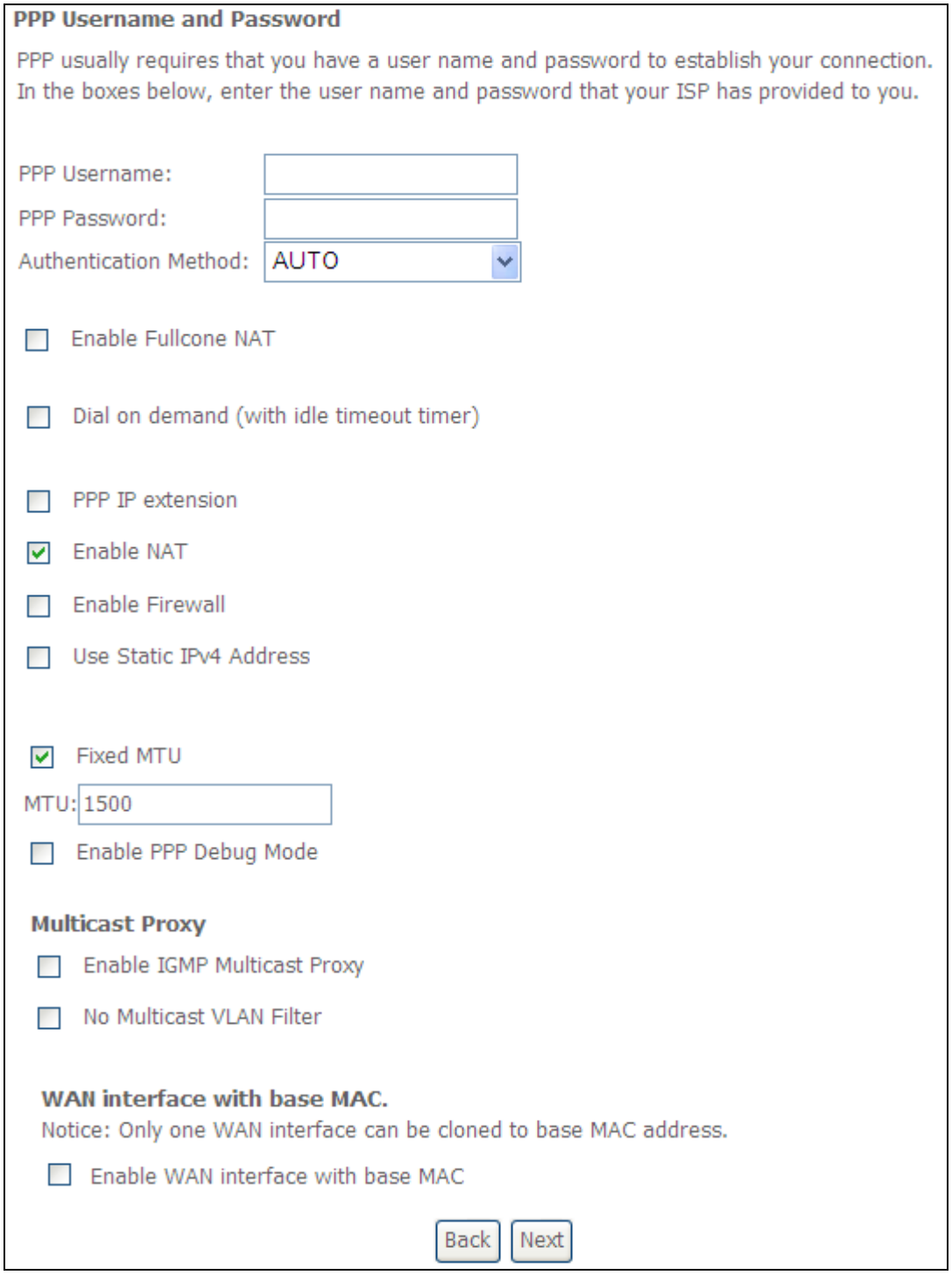
NOTE:	If this bridge connection is your only WAN service, the AR-5389 will be inaccessible for remote management or technical support from the WAN.

E2.4 PPP over ATM (PPPoA)



STEP 1: Click **Next** to continue.

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
PPP IP extension
Enable NAT
Enable Firewall
Use Static IPv4 Address
Fixed MTU
MTU:
1500
Enable PPP Debug Mode
Multicast Proxy
Enable IGMP Multicast Proxy
No Multicast VLAN Filter
WAN interface with base MAC.
Notice: Only one WAN interface can be cloned to base MAC address.
Enable WAN interface with base MAC
Back
Next

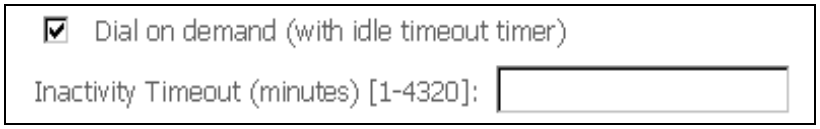
PPP SETTINGS

The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The AR-5389 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in Section 3.2.

Fixed MTU
Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

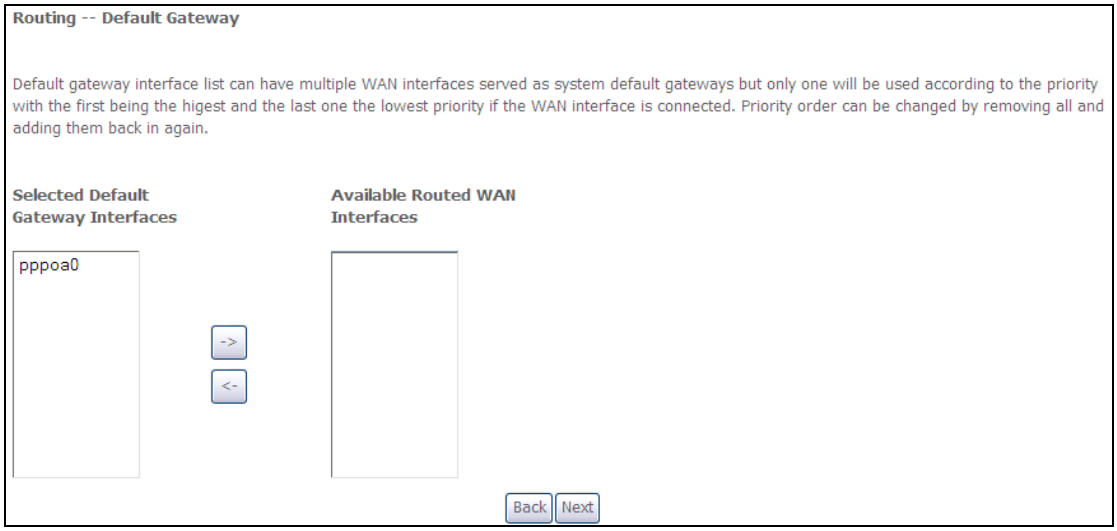
ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

ENABLE IGMP MULTICAST Proxy
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

NO MULTICAST VLAN FILTER
Tick the checkbox ☑ to have the multicast packets bypass the VLAN filter.

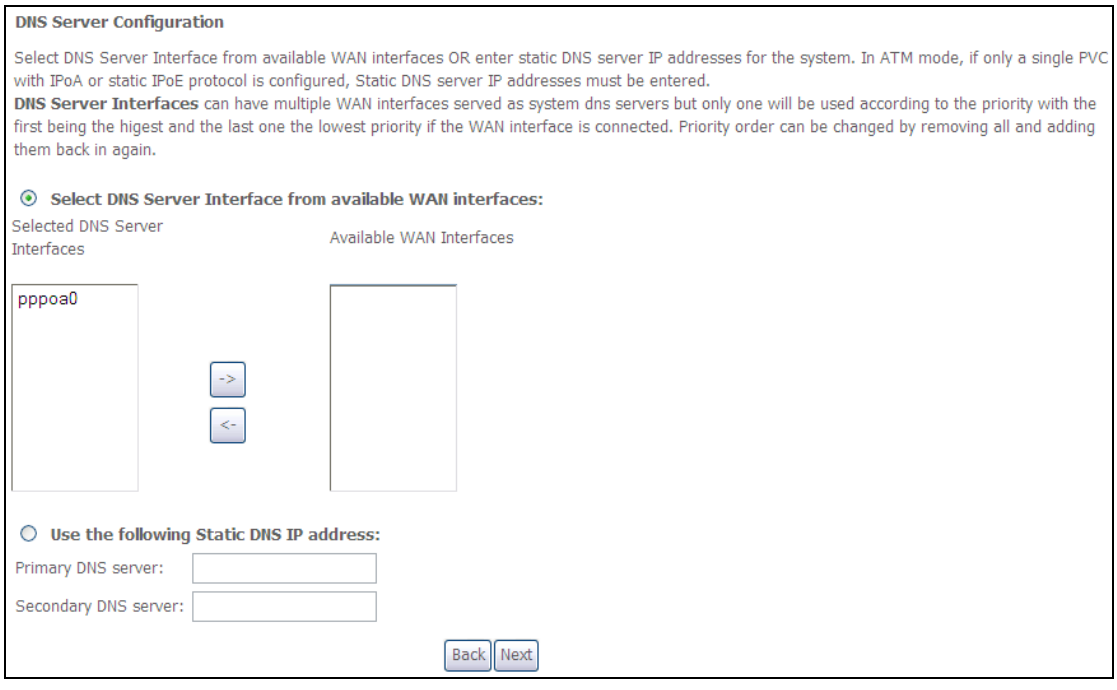
Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 3: Choose an interface to be the default gateway.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
pppoa0
->
<-
Back
Next

Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Choose an interface to be the default gateway.


DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
pppoa0
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

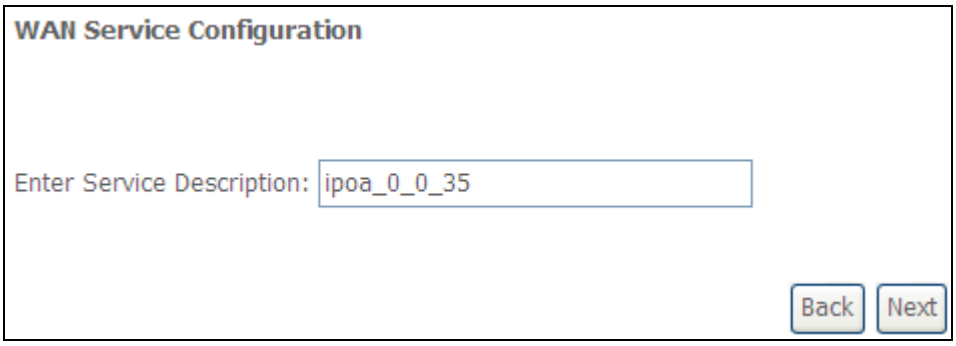
Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoA
NAT: Enabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

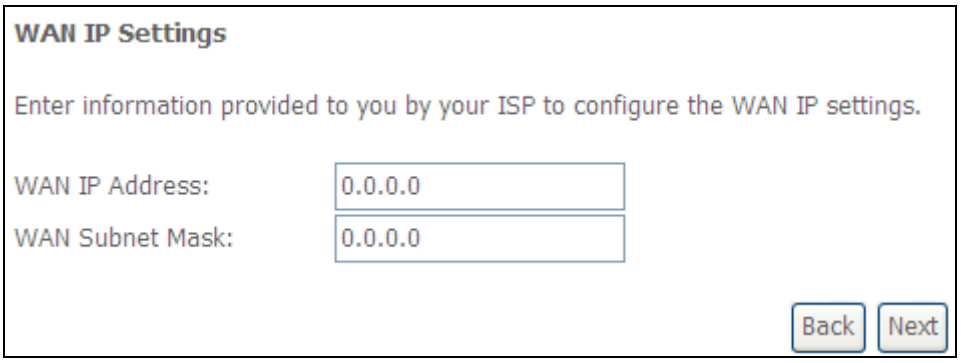
After clicking **Apply / Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

E2.5 IP over ATM (IPoA)

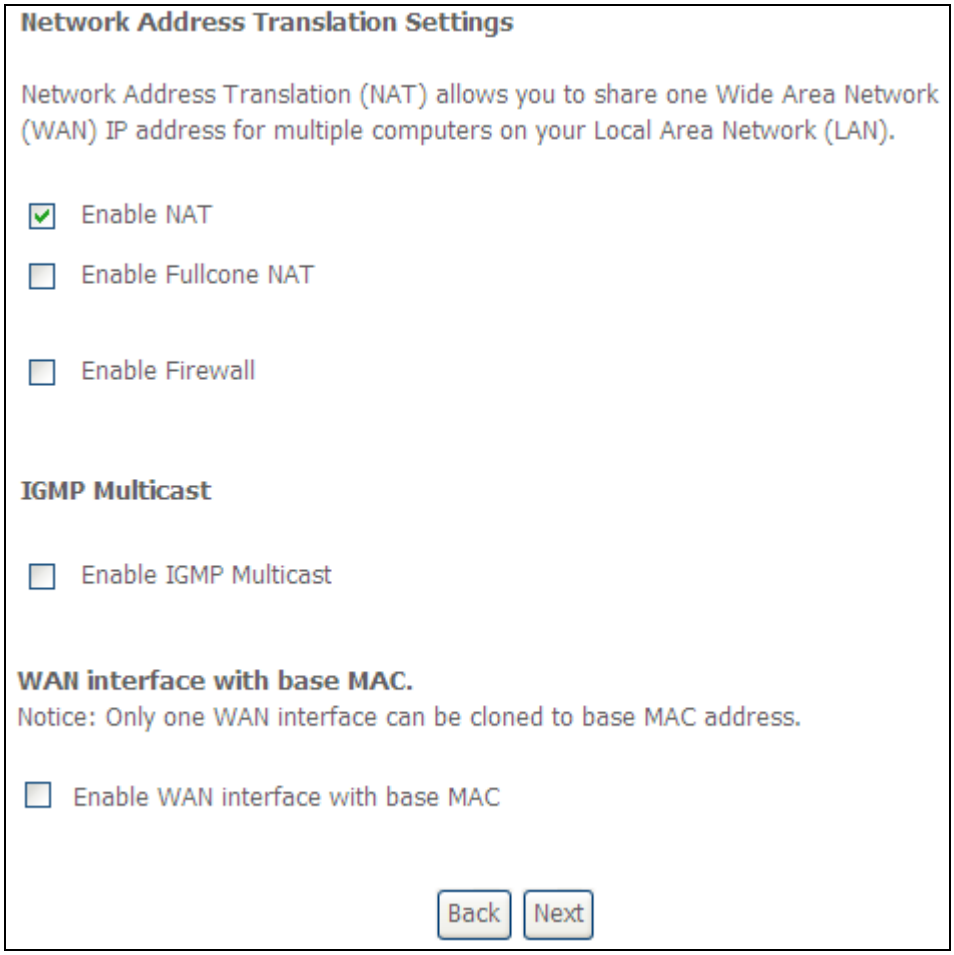


STEP 1: Click **Next** to continue.

STEP 2: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.



STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Fullcone NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast
WAN interface with base MAC.
Notice: Only one WAN interface can be cloned to base MAC address.
Enable WAN interface with base MAC
Back
Next

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

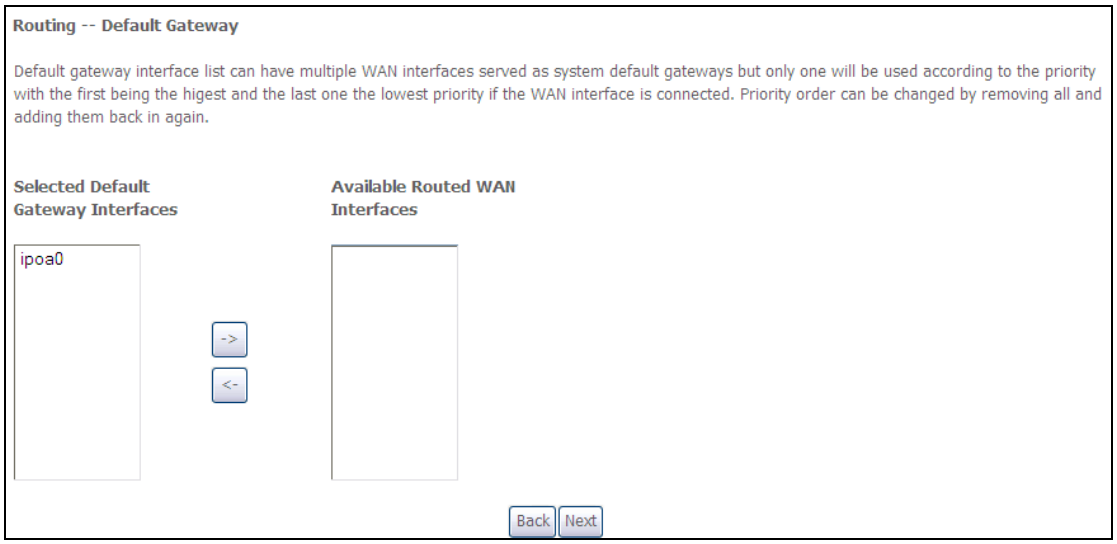
ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host by sending a packet to the mapped external address.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

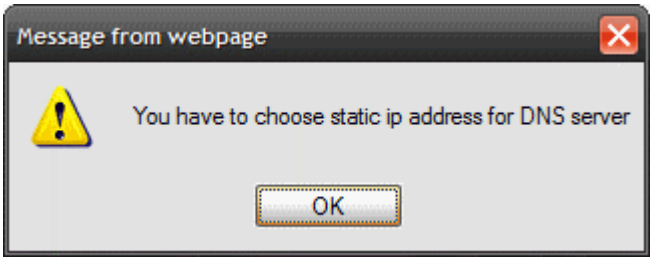
Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 4: Choose an interface to be the default gateway.

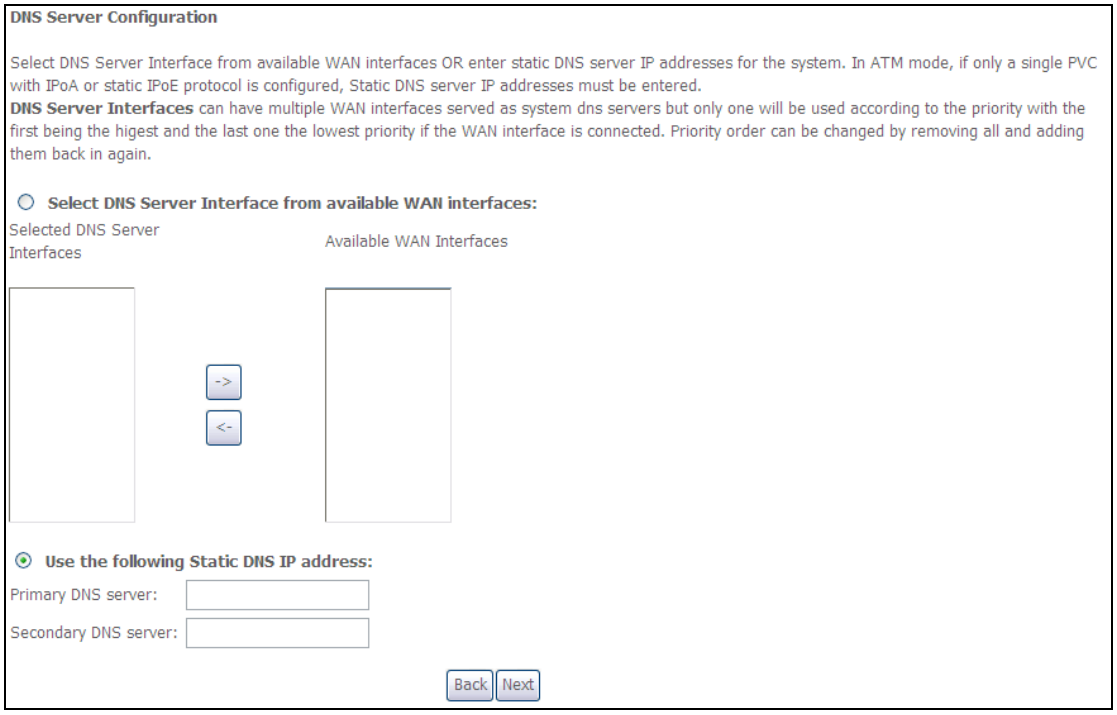

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ipoa0
->
<-
Back
Next

Click **Next** to continue or click **Back** to return to the previous step.

NOTE: If the DHCP server is not enabled on another WAN interface then the following notification will be shown before the next screen.

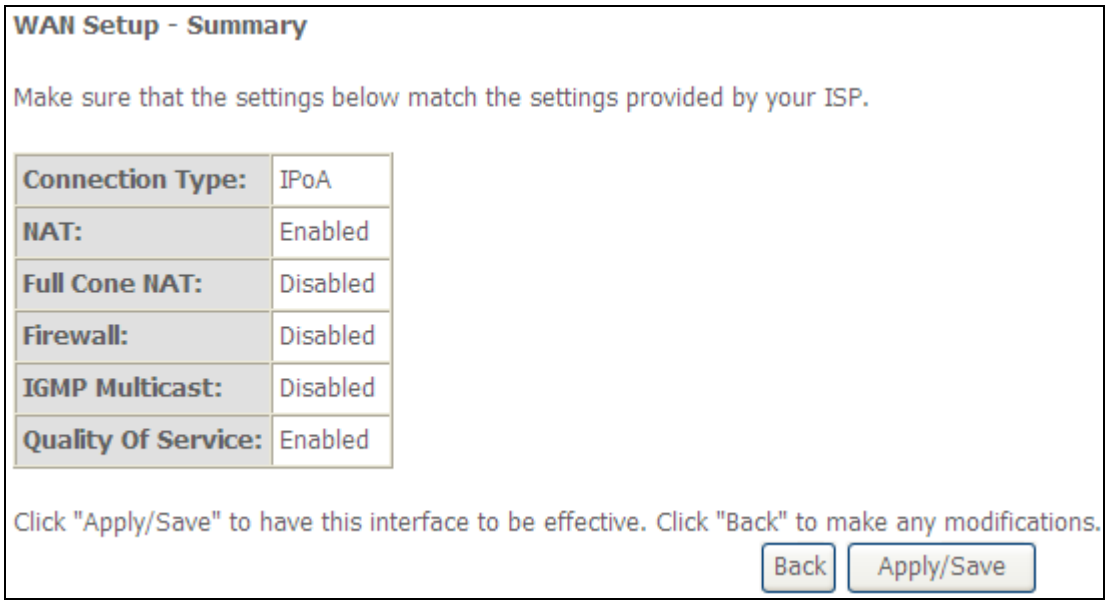


STEP 5: Choose an interface to be the default gateway.


DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Select DNS Server Interface from available WAN interfaces:
Selected DNS Server Interfaces
Available WAN Interfaces
->
<-
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoA
NAT: Enabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.